VASCO
THE AUTHENTICATION COMPANY

DIGIPASS
authentication

DIGIPASS® Authentication for OWA Forms User Manual

3.4

Disclaimer of Warranties and Limitations of Liabilities

The Product is provided on an 'as is' basis, without any other warranties, or conditions, express or implied, including but not limited to warranties of merchantable quality, merchantability of fitness for a particular purpose, or those arising by law, statute, usage of trade or course of dealing. The entire risk as to the results and performance of the product is assumed by you. Neither we nor our dealers or suppliers shall have any liability to you or any other person or entity for any indirect, incidental, special or consequential damages whatsoever, including but not limited to loss of revenue or profit, lost or damaged data of other commercial or economic loss, even if we have been advised of the possibility of such damages or they are foreseeable; or for claims by a third party. Our maximum aggregate liability to you, and that of our dealers and suppliers shall not exceed the amount paid by you for the Product. The limitations in this section shall apply whether or not the alleged breach or default is a breach of a fundamental condition or term, or a fundamental breach. Some states/countries do not allow the exclusion or limitation or liability for consequential or incidental damages so the above limitation may not apply to you.

Copyright

Trademarks

VASCO®, VACMAN®, IDENTIKEY®, aXsGUARD™, DIGIPASS®, CertiID™, and the Vasco 'V' logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries.

Date: 2012-03-02

Table of Contents

Illustration Index

Index of Tables

1 Introduction

Welcome to the DIGIPASS Authentication for OWA Forms User Manual. This document provides information you will need to install and use DIGIPASS Authentication for OWA Forms.

This guide provides information about:

- the DIGIPASS Authentication for OWA Forms features and functionalities
- how to install DIGIPASS Authentication for OWA Forms
- how to configure DIGIPASS Authentication for OWA Forms
- how to troubleshoot possible issues that may occur when working with DIGIPASS Authentication for OWA Forms

This guide does not provide:

- detailed information about IDENTIKEY Server or aXsGUARD Identifier (refer to the respective product documentation)

1.1 About This Manual

1.1.1 How to Use This Manual

You can use this manual in different ways, depending on your skill and knowledge level. You can read it from the beginning to the end (highly recommended for novice users), you can browse through the chapter abstracts and read specifically the chapters relevant to your needs, or you can search by key words in the index, if you need to find certain references quickly.s

If you need to…	Refer to
...get an overview of the DIGIPASS Authentication for OWA Forms architecture and features	2 DIGIPASS Authentication for OWA Forms Overview
...get instructions to install DIGIPASS Authentication for OWA Forms	3 Installing DIGIPASS Authentication for OWA Forms -AND- 5 Post-Installation Tasks
...configure DIGIPASS Authentication for OWA Forms and/or Exchange	4 Configuring DIGIPASS Authentication for OWA Forms
...troubleshoot your DIGIPASS Authentication for OWA Forms installation	6 Troubleshooting

1.1.2 Document Conventions

The following typographic style conventions are used throughout this document.

Typography	Meaning
Boldface	Names of user interface widgets, e.g. the **OK** button
Blue	Values for options; placeholders for information or parameters that you provide, e.g. select Server name in the list box.
UPPERCASE	Keyboard keys, e.g. CTRL for the Control key
`Monospace`	Commands you are supposed to type in or are displayed in a command prompt shell, including directories and filenames; API functions and source code examples
blue, underlined	Internet links

The following visual hint colour schemes are used throughout this document.

TIP
Tips contain supplementary information that is not essential to the completion of the task at hand, including explanations of possible results or alternative methods.

NOTE
Notes contain important supplementary information.

CAUTION
Cautions contain warnings about possible data loss, breaches of security, or other more serious problems.

1.1.3 Providing Feedback

Every effort has been made to ensure the accuracy and usefulness of this manual. However, as the reader of this documentation, *you* are our most important critic and commentator. We appreciate your judgment and would like you to write us your opinions, suggestions, critics, questions, and ideas. Please send your commentary to: documentation@vasco.com.

To recognize the particular document you are referring to, please include the following information in your subject header: DAOWAF-UM-02032012

Please note that product support is not offered through the above mail address.

2 DIGIPASS Authentication for OWA Forms Overview

This chapter gives an overview of the DIGIPASS Authentication for OWA Forms features and functionalities. It provides a list of terms you should be familiar with when working with DIGIPASS Authentication for OWA Forms and outlines various authorization scenarios.

This chapter covers the following topics:

- General Overview
- DIGIPASS Authentication Plug-In Terminology
- Authentication Methods
- Server Connection Management
- Tracing

2.1 General Overview

The **DIGIPASS Authentication Plug-In** is an add-on for Internet Information Services (IIS) and can be configured to intercept authentication requests to Web sites using the HTTP forms authentication mechanism. It allows users to use one-time passwords (OTPs) instead of static passwords. The plug-in intercepts authentication requests, validates the OTP, and replaces it with the static password expected by the back-end. The OTPs are validated using an IDENTIKEY Server or aXsGUARD Identifier.

The **DIGIPASS Authentication Plug-In** is a native module for IIS 7.x.

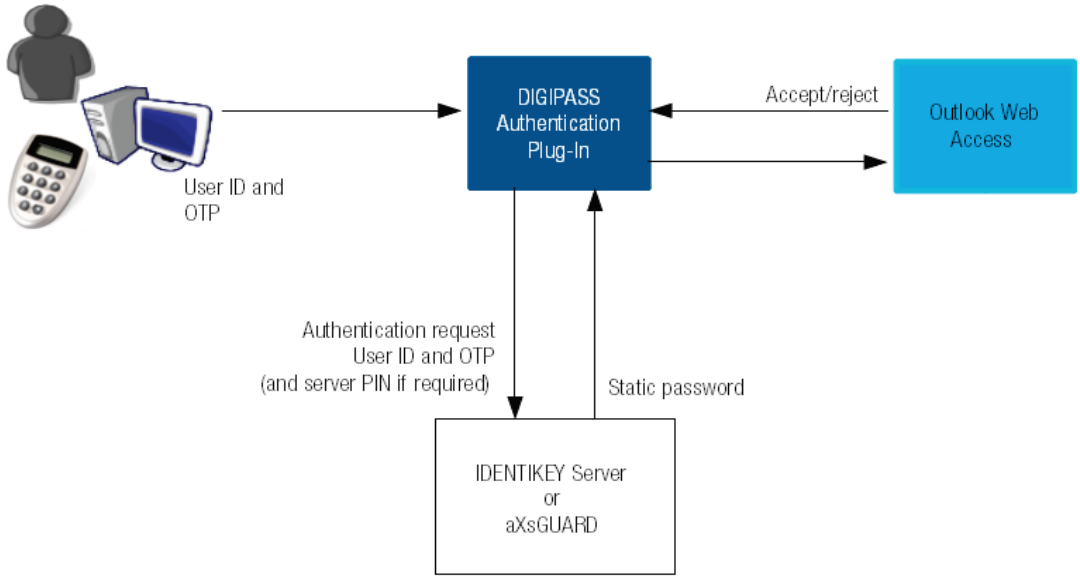

Figure 1: DIGIPASS Authentication for OWA Forms Overview

2.2 DIGIPASS Authentication Plug-In Terminology

The following definitions describe how these terms are used in this document. They are also used in other IIS plug-in manuals.

Authentication server

The term authentication server refers to the component to which the **DIGIPASS Authentication Plug-In** sends authentication requests. This component is:

- For IDENTIKEY Server, the IDENTIKEY Server service or daemon
- For aXsGUARD Identifier, the IDENTIKEY Server daemon

Basic authentication

A method of authentication that uses the HTTP basic authentication mechanism. This uses a login pop-up box provided by the browser.

Client record

The client record is the record defined in the authentication server's data store, to represent an installed instance of the **DIGIPASS Authentication Plug-In**.

It is used for the following main purposes:

- To indicate that the authentication server is permitted to process a request from that client
- To specify a policy to be used to process the request
- To hold a license key for the **DIGIPASS Authentication Plug-In**

Forms authentication

The method of authentication where a Web site provides its own login page.

DIGIPASS Authentication Plug-In

General term for a plug-in to IIS to allow DIGIPASS authentication to take place.

2.3 Authentication Methods

See the Product Guide for your authentication server product for detailed information on login methods and options.

Response-only login

Users log in via the current login page with their user name and a one-time password (OTP).

One-step challenge/response login

A random challenge - of a length configured for all users in the authentication server's policy - is displayed on the login page. Users log in with their user name and DIGPASS response to the displayed challenge. This requires modification of the current login page used by OWA. For more information, refer to Section 5.2 Setting Up the One-Step Challenge/Response Login.

Two-step challenge/response login

After the login page, the **DIGIPASS Authentication Plug-In** redirects users to a 'Challenge page' where a random challenge – of the length required by the user's DIGPASS – is displayed. The user must enter a response to the challenge in order to complete the login.

A challenge page template must be used with this feature. A default template is provided. It can be used without modification or it can be customized to match your preferred look and feel. For more information, refer to Section 5.4 Creating a Two-Step Challenge/Response Template.

Virtual DIGIPASS login

Users logging in with a Virtual DIGIPASS use a similar process to the two-step challenge/response login. If the user has a primary Virtual DIGIPASS assigned, or requests use of the backup Virtual DIGIPASS feature during the first step, an OTP will be sent to the user's mobile phone via text message. The user is then redirected by the **DIGIPASS Authentication Plug-In** to the challenge page to enter the OTP.

This uses the same challenge template used in the two-step challenge/response login.

2.4 Server Connection Management

The **DIGIPASS Authentication Plug-In** provides flexibility in managing connections to multiple primary and/or backup authentication servers. This allows redundancy and load sharing over multiple servers.

2.4.1 Connection Profiles

Two connection profiles are available:

Primary

The server(s) to which the **DIGIPASS Authentication Plug-In** will first attempt to connect, using a round-robin scheme.

Backup

Backup servers will be used if load sharing is enabled and the primary server(s) are busy.

2.4.2 Connection Options

Maximum connections

The maximum number of connections that the **DIGIPASS Authentication Plug-In** may have open to the authentication server at one time.

Timeout

The time that the **DIGIPASS Authentication Plug-In** should wait for a reply from the authentication server.

Reconnect interval

If the **DIGIPASS Authentication Plug-In** cannot connect to an authentication server, it will make another connection attempt to this server only after a time period defined by the reconnect interval. If other servers are configured, connection attempts to these servers are made in the meantime.

2.4.3 Standard Server Setup

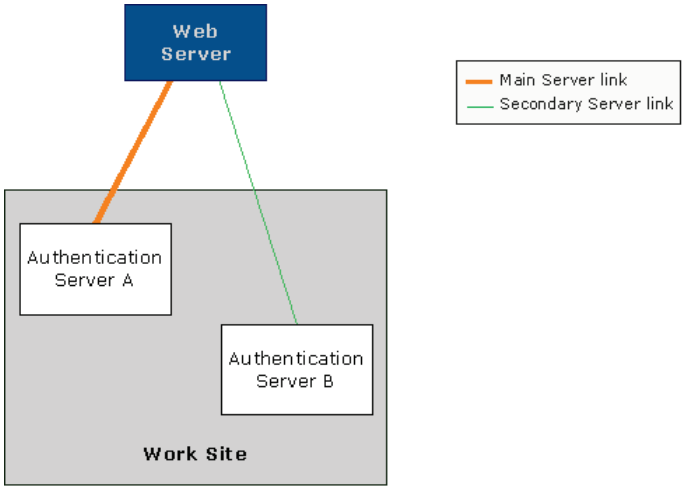

Figure 2: Standard Server Connection Configuration

This setup uses one main authentication server to handle requests from the Web server, with a backup authentication server for use when the main server is busy or unavailable.

2.5 Tracing

The **DIGIPASS Authentication Plug-In** allows use of a trace file to record plug-in activity, e.g. for troubleshooting. This will include errors that have been encountered, warnings, and general information about performed authentication requests.

The level of tracing that the **DIGIPASS Authentication Plug-In** employs depends on its configuration settings.

CAUTION
Enabling full tracing should only be done for troubleshooting purposes. There are no limits set on the size of the tracing file, so if the option is left on too long on a high-load system the file may dramatically slow down or crash Windows, due to excessive I/O or filling up the hard drive.

Because there are no size limitations set on the trace file, it is not recommended that you have tracing permanently enabled. If your system is set up with tracing always enabled, ensure that the file size does not cause problems by deleting or archiving it whenever it gets too large.

Basic tracing includes:

- Error messages
- Warnings
- High-level information about plug-in activity

Full tracing includes:

- Error messages
- Warnings
- High-level information about plug-in activity
- Detailed information about plug-in activity

NOTE
The **DIGIPASS Authentication Plug-In** will require permissions for the directory in which the tracing file is kept. See Section 6.1.2 Checking Permissions for more information.

3 Installing DIGIPASS Authentication for OWA Forms

This chapter contains instructions to install DIGIPASS Authentication for OWA Forms. It lists system and other requirements, as well as pre-installation settings and tasks. Be sure to check that all system requirements and pre-installation tasks have been met before installing the **DIGIPASS Authentication Plug-In**. This will help ensure a smooth, trouble-free installation and integration process.

This chapter covers the following topics:

- System Requirements
- Pre-Installation Tasks
- Installing DIGIPASS Authentication for OWA Forms
- Using the DIGIPASS Authentication for OWA Forms Configuration Wizard

3.1 System Requirements

3.1.1 Software Requirements

To install DIGIPASS Authentication for OWA Forms you need:

- An authentication server running on another machine. This should be one of the following:
  - IDENTIKEY Server 3.1 or later – IDENTIKEY Server component
  - aXsGUARD Identifier 3.1.3.x or later
- Internet Information Services (IIS) 7 or 7.5
- Windows Server 2008 with SP1 (or later), 32- and 64-bit
  -OR-
  Windows Server 2008 R2 with SP1 (or later), 64-bit
- MS Exchange 2007 or 2010 using Outlook Web Access in forms authentication mode and SSL
- The user must have administration rights on the installation machine.

3.2 Pre-Installation Tasks

Before installing the **DIGIPASS Authentication Plug-In**, there are several tasks which need to be completed. Performing these tasks (where applicable) will assist in a quick, smooth installation process.

3.2.1 Installing the Authentication Server

An authentication server should be installed on the network before the **DIGIPASS Authentication Plug-In** is installed. See Section 3.1 System Requirements for compatible servers and 4.4 Configuring the Authentication Server for configuration recommendations.

CAUTION

If the users are Active Directory users on a Windows platform, it is recommended that the **Use Windows user name resolution** feature on the authentication server is enabled. This uses Windows functions to identify user IDs as Windows user accounts, including the domain to which the account belongs.

This feature is not available on Linux platforms or the aXsGUARD Identifier.

If the **Use Windows user name resolution** feature is disabled, it is essential that users always use the same login name. If they try to log in using a different form of their Windows account name, their login will be rejected, unless a second DIGIPASS user account has been created.

3.2.2 IIS and Exchange

Ensure IIS and Exchange are installed and working correctly. The **DIGIPASS Authentication Plug-In** must be installed on the IIS server where Outlook Web Access is running.

3.2.3 Information Needed

Before you begin installation of the **DIGIPASS Authentication Plug-In**, ensure that you have the following information easily accessible, as you will need to enter this during the installation.

- IP address and port number of the authentication server. To check this, open the authentication server configuration and check the **Component location** and **SEAL port** fields.
- Source IP address on the local machine to use when connecting to the authentication server (if multiple IP addresses are configured for this machine, as this affects licensing – see below).

3.2.4 Licensing

The authentication server will associate authentication requests from each incoming IP address with a different client record. Your **DIGIPASS Authentication Plug-In** license will be tied to that IP address. The IP address of the computer where IIS is running must match the IP address of the license, or authentication will not be possible.

3.3 Installing DIGIPASS Authentication for OWA Forms

➢ To install DIGIPASS Authentication for OWA Forms

1. Locate DIGIPASS Authentication for OWA Forms.msi and start the installation process.

Figure 3: Installing DIGIPASS Authentication for OWA Forms (1)

2. Read the license agreement text, select **I accept the terms in the license agreement**, and click **Next**.

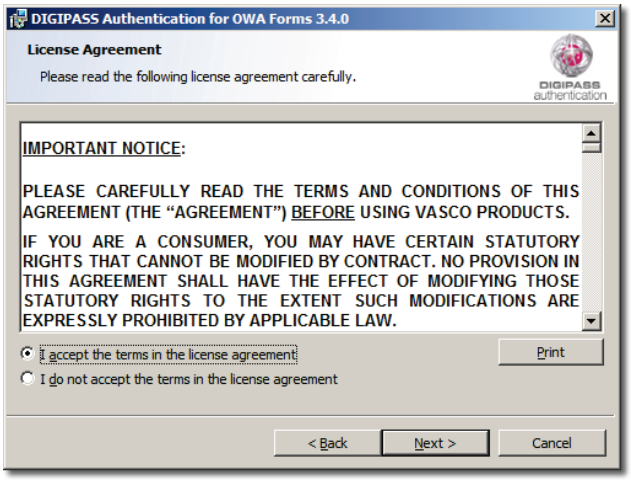

Figure 4: Installing DIGIPASS Authentication for OWA Forms (2)

3. Specify the destination folder for DIGIPASS Authentication for OWA Forms and click **Next**.
   The default destination folder (referred to as <INSTALLATION DIRECTORY> in this document) is

C:\Program Files\VASCO\DIGIPASS Authentication for OWA Forms.

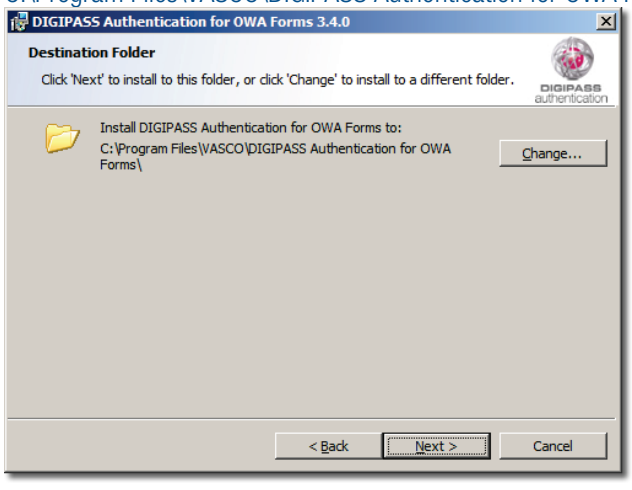

Figure 5: Installing DIGIPASS Authentication for OWA Forms (3)

4. Click **Install** to start the installation.

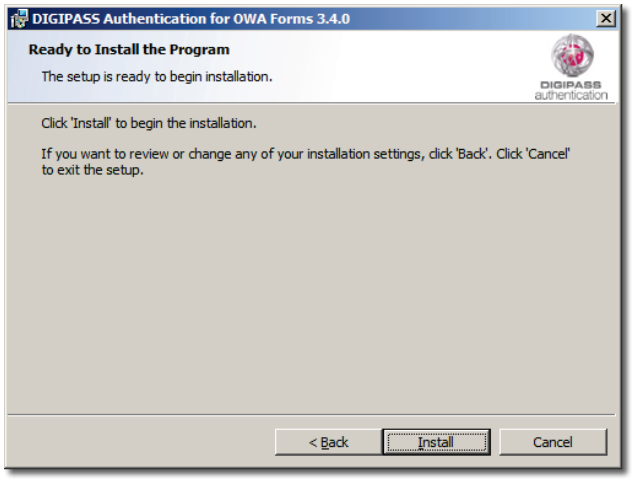

Figure 6: Installing DIGIPASS Authentication for OWA Forms (4)

5. After successful installation, click **Finish** to exit the setup program.
   The DIGIPASS Authentication for OWA Forms configuration wizard is started.

3.4 Using the DIGIPASS Authentication for OWA Forms Configuration Wizard

After you have finished the installation wizard, the DIGIPASS Authentication for OWA Forms configuration wizard is started automatically. Go through the wizard to define the basic settings for using the **DIGIPASS Authentication Plug-In**. Once the wizard is complete, the **DIGIPASS Authentication Plug-In**'s Settings.xml is filled with the default configuration for OWA forms, and the **DIGIPASS Authentication Plug-In** is ready for use.

For further configuration options and to change your initial settings, use the **DIGIPASS Authentication Plug-In Configuration Center** or edit Settings.xml. For more information, refer to Sections 4.1 Using the DIGIPASS Authentication Plug-In Configuration Center and 4.2 Editing the Configuration File.

3.4.1 Configuring DIGIPASS Authentication for OWA Forms

➢ To configure DIGIPASS Authentication for OWA Forms

1. When the wizard is started, click **Next**.
   The configuration wizard is started automatically after you have completed the installation wizard. Afterwards, if you want to modify your settings using the wizard, select **Start > All Programs > VASCO > DIGIPASS Authentication for OWA Forms > Configuration Wizard**.

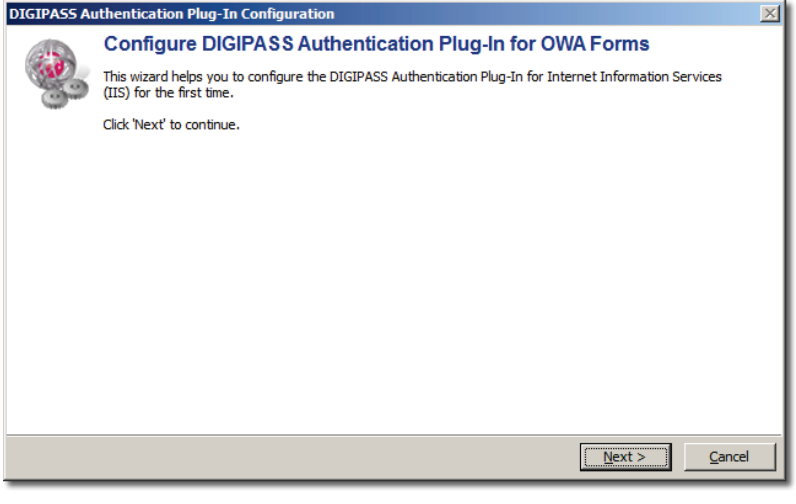

Figure 7: Using the Configuration Wizard (1)

2. Specify the IP address and SEAL port of the authentication server.

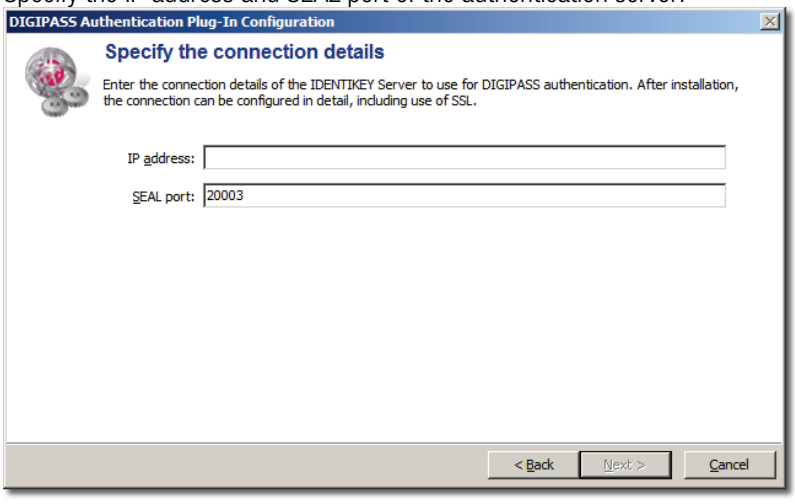

Figure 8: Using the Configuration Wizard (2)

3. Select an IP address from the list, which contains IP addresses assigned to the current machine. The **DIGIPASS Authentication Plug-In** will use the selected IP address exclusively.
As VASCO component licensing operates on IP address, this ensures that the **DIGIPASS Authentication Plug-In** will only use up one component license slot. For more information, refer to Section 3.2.4 Licensing.

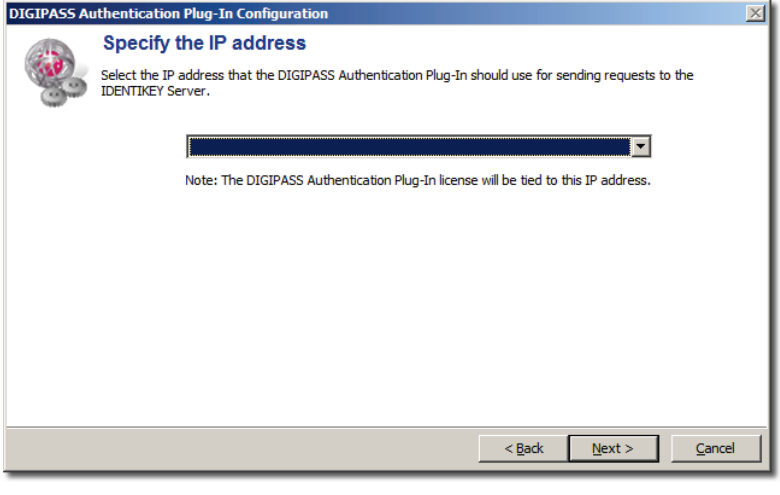

Figure 9: Using the Configuration Wizard (3)

4. Specify whether to create an IDENTIKEY client record.

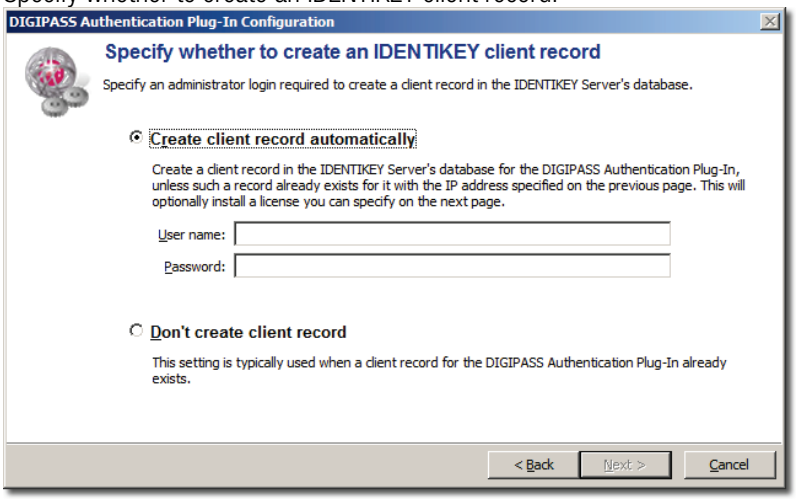

Figure 10: Using the Configuration Wizard (4)

- Select **Create client record automatically** if you want to specify the administrator login for the authentication server to register the **DIGIPASS Authentication Plug-In** as a client in the authentication server database.
  Provide the user name and password to allow administrative access to the authentication server.
- Select **Don't create client record** if the client record for the **DIGIPASS Authentication Plug-In** already exists in the authentication server database, or you prefer to create it manually.

5. Specify a license key. This option is available only if you selected **Create client record automatically**.

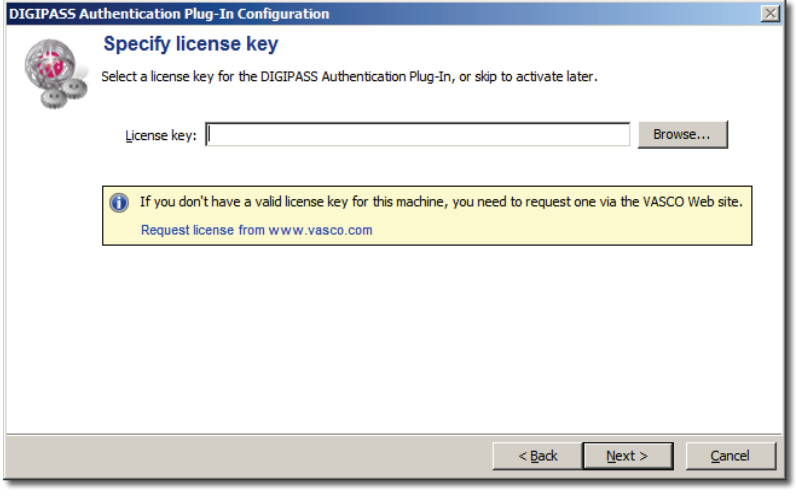

Figure 11: Using the Configuration Wizard (5)

- Browse to the license.dat file to load the license key from where you saved it on your local machine and click **Open** to load the license key from the file.

- If you do not already have a license key file, click on **Request license from www.vasco.com**. This will take you to the VASCO Web site, where you can request a license key and save it to your local machine.

6. Review the settings you have specified and click **Finish**.

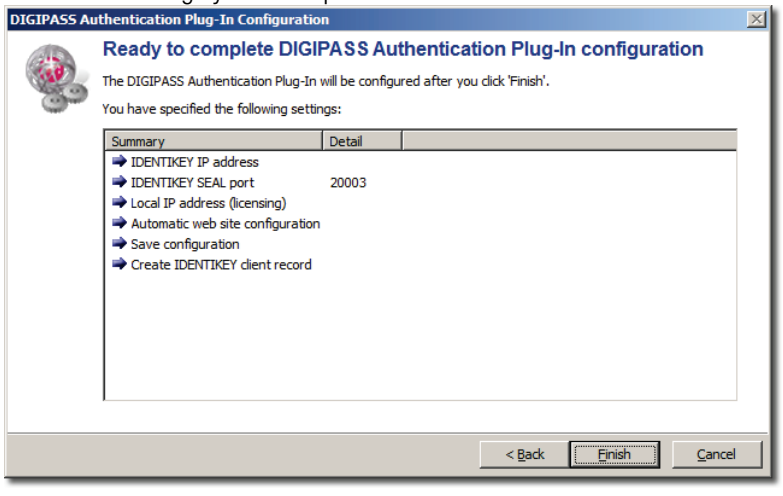

Figure 12: Using the Configuration Wizard (6)

4 Configuring DIGIPASS Authentication for OWA Forms

This chapter describes how to configure the **DIGIPASS Authentication Plug-In**. Configuration settings can be modified in two ways. The easiest method is via the **DIGIPASS Authentication Plug-In Configuration Center** – a graphical interface that allows you to make changes with a few mouse clicks. Advanced users may prefer to edit the configuration file directly.

This chapter covers the following topics:

- Using the DIGIPASS Authentication Plug-In Configuration Center
- Editing the Configuration File
- Configuring Exchange to Work with the DIGIPASS Authentication Plug-In
- Configuring the Authentication Server

4.1 Using the DIGIPASS Authentication Plug-In Configuration Center

A graphical user interface (GUI) called **DIGIPASS Authentication Plug-In Configuration Center**, is available for use in configuring the **DIGIPASS Authentication Plug-In**. This provides a simple, intuitive way to set up the **DIGIPASS Authentication Plug-In** to work with your current system.

If this is the first time you have opened the **DIGIPASS Authentication Plug-In Configuration Center** and the configuration file has not been edited, the values you will see are those entered when the wizard was last run.

4.1.1 Starting DIGIPASS Authentication Plug-In Configuration Center

➢ To start DIGIPASS Authentication Plug-In Configuration Center

- Select **Start > All Programs > VASCO > DIGIPASS Authentication for OWA Forms > Configuration Center**.
  -OR-
  Open Windows Explorer and launch <INSTALLATION DIRECTORY>\VdsConfig32.exe (32-bit systems) or <INSTALLATION DIRECTORY>\VdsConfig64.exe (64-bit systems).

4.1.2 Configuring Servers and Connections

➢ To add and configure authentication servers

1. Start **DIGIPASS Authentication Plug-In Configuration Center** and select **Servers and Connections**.

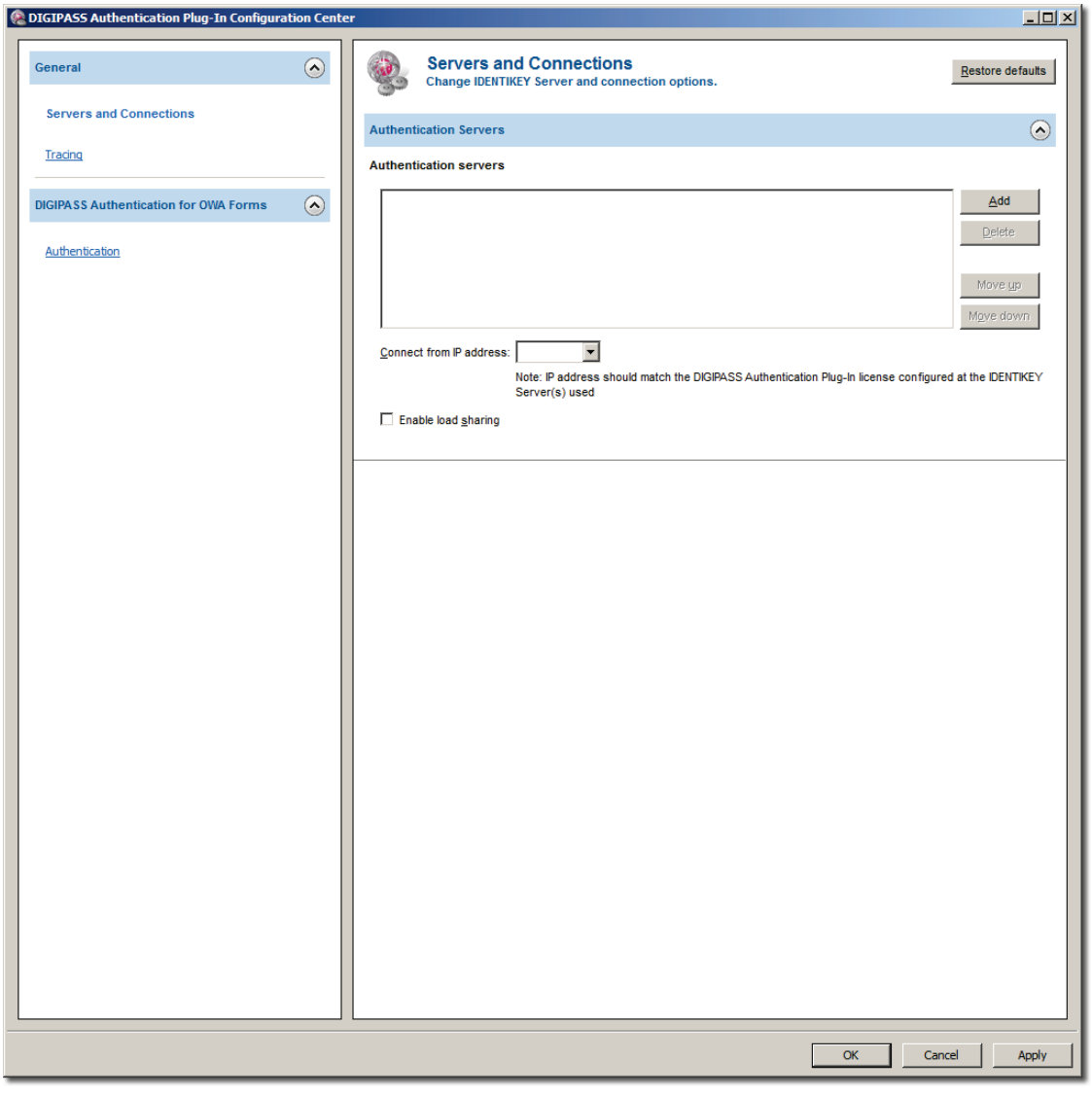

Figure 13: Configuring Servers and Connections (1)

2. Do one of the following:
   - Click **Add** if you want to add a new authentication server.
   - To modify the settings for an authentication server, select the server from the **Authentication servers** list.

The **Configuration for <AUTHENTICATION SERVER>** section appears.

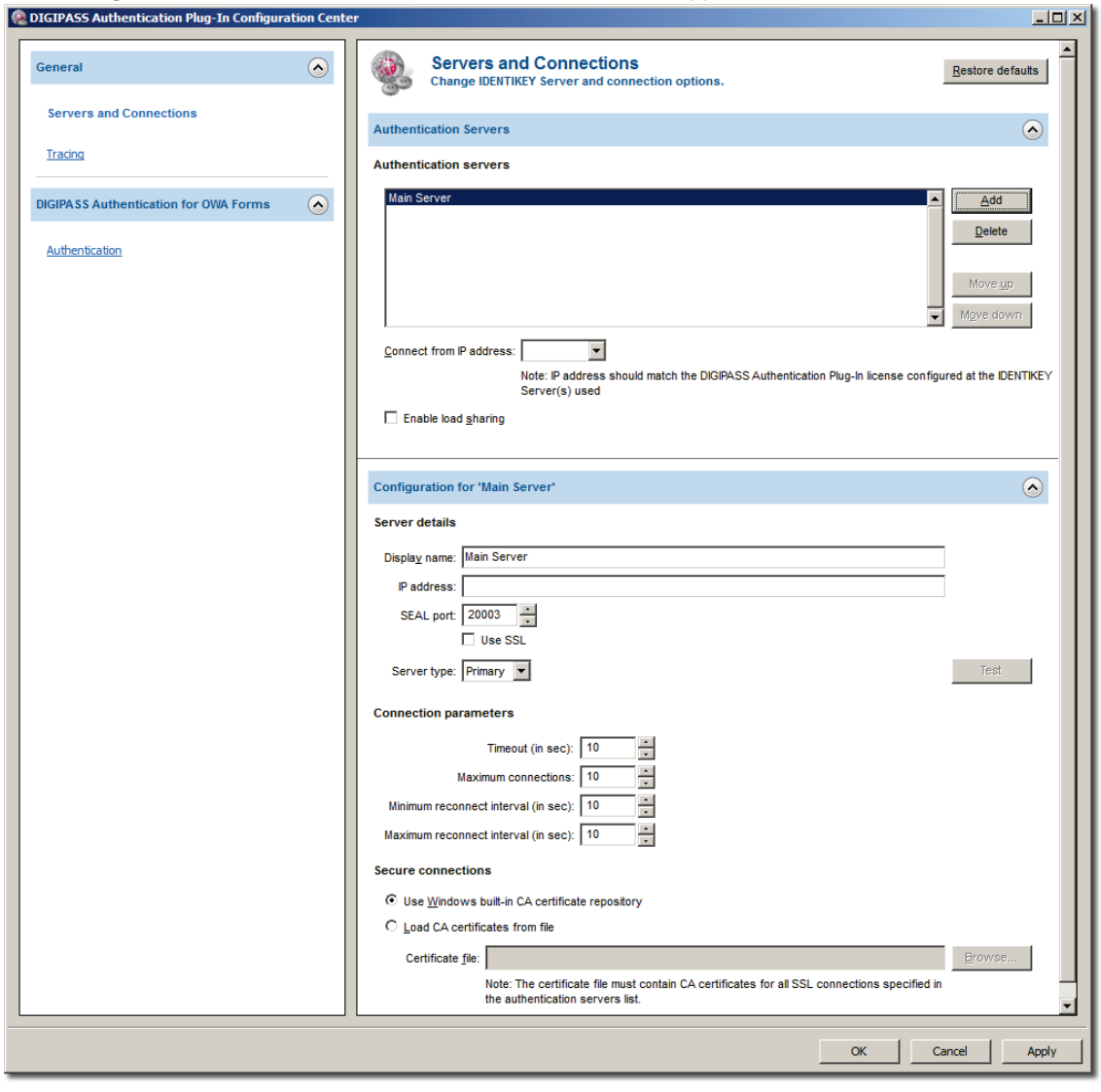

Figure 14: Configuring Servers and Connections (2)

3. Select an IP address from the **Connect from IP address** list from which to connect to the authentication server.

4. Select **Enable load sharing** if you want to use a backup server. For more information, refer to Section 2.4.1 Connection Profiles.

5. Specify the server settings as needed.

   - **Display name**: Type a name for the authentication server in this field. This name is then used to distinguish the authentication server in the **Authentication servers** list, but has no effect on the behaviour of the **DIGIPASS Authentication Plug-In**.

   - **IP address**: Type the IP address for the authentication server.

- **SEAL port**: Type the port for the authentication server. The default port is 20003 for standard, and 20004 for SSL connections.
- **Use SSL**: Select this if you want to use SSL when connecting to the authentication server. This option is only available for IDENTIKEY Server 3.1 or later.
- **Server type**: Select the server type. For more information, refer to Section 2.4.1 Connection Profiles.

6. (OPTIONAL) Click **Test** to test if a connection to the authentication server can be established. A message will appear indicating if the test was successful.
7. Specify the connection parameters as needed.
   - **Timeout (in sec)**: Specify a timeout period in seconds.
   - **Maximum connections**: Specify the maximum number of concurrent connections to be made from the **DIGIPASS Authentication Plug-In** to the authentication server.
   - **Minimum reconnect interval (in sec)**: Specify the minimum amount of time that the **DIGIPASS Authentication Plug-In** should wait before attempting to reconnect to the authentication server.
   - **Maximum reconnect interval (in sec)**: Specify the maximum amount of time that the **DIGIPASS Authentication Plug-In** should wait before attempting to reconnect to the authentication server.
8. Specify secure connection settings.
   - Select **Use Windows built-in CA certificate repository** if you want to trust the certificate authorities in the Windows CA certificate repository.
   - Select **Load CA certificates from file** if you want to use your own CA certificate list. Browse to the certificate file and click **Open**.
9. Click **Apply** for your changes to take effect.

4.1.3 Configuring Authentication Settings

➢ To configure authentication settings

1. Start **DIGIPASS Authentication Plug-In Configuration Center** and select **Authentication**.

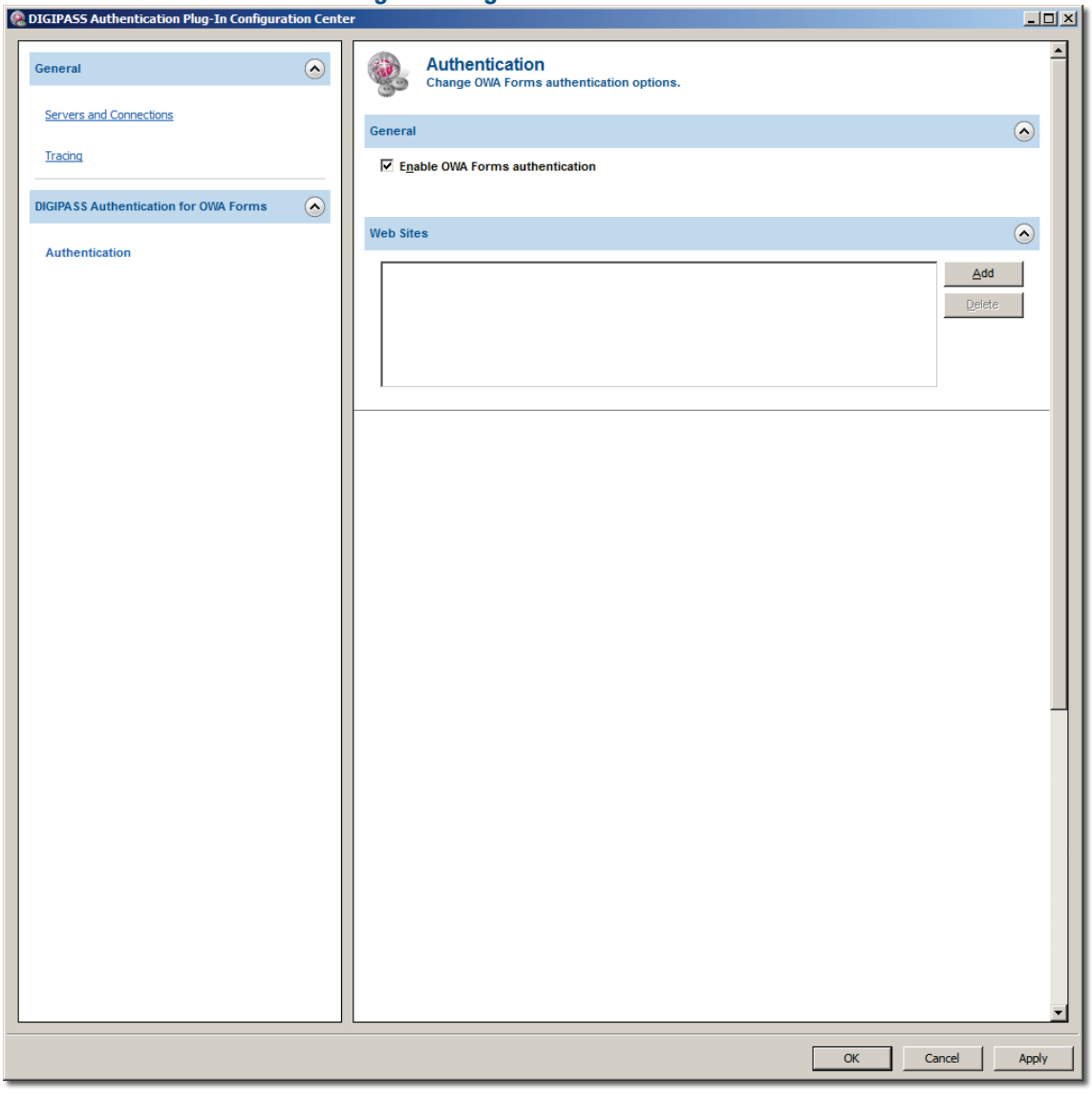

Figure 15: Configuring Authentication Settings (1)

2. Select **Enable OWA Forms authentication** to allow the **DIGIPASS Authentication Plug-In** to intercept authentication requests using the authentication server.
3. Do one of the following:
   - Click **Add** if you want to add a new Web site.

- To modify the settings for a Web site, select the Web site from the **Web Sites** list.

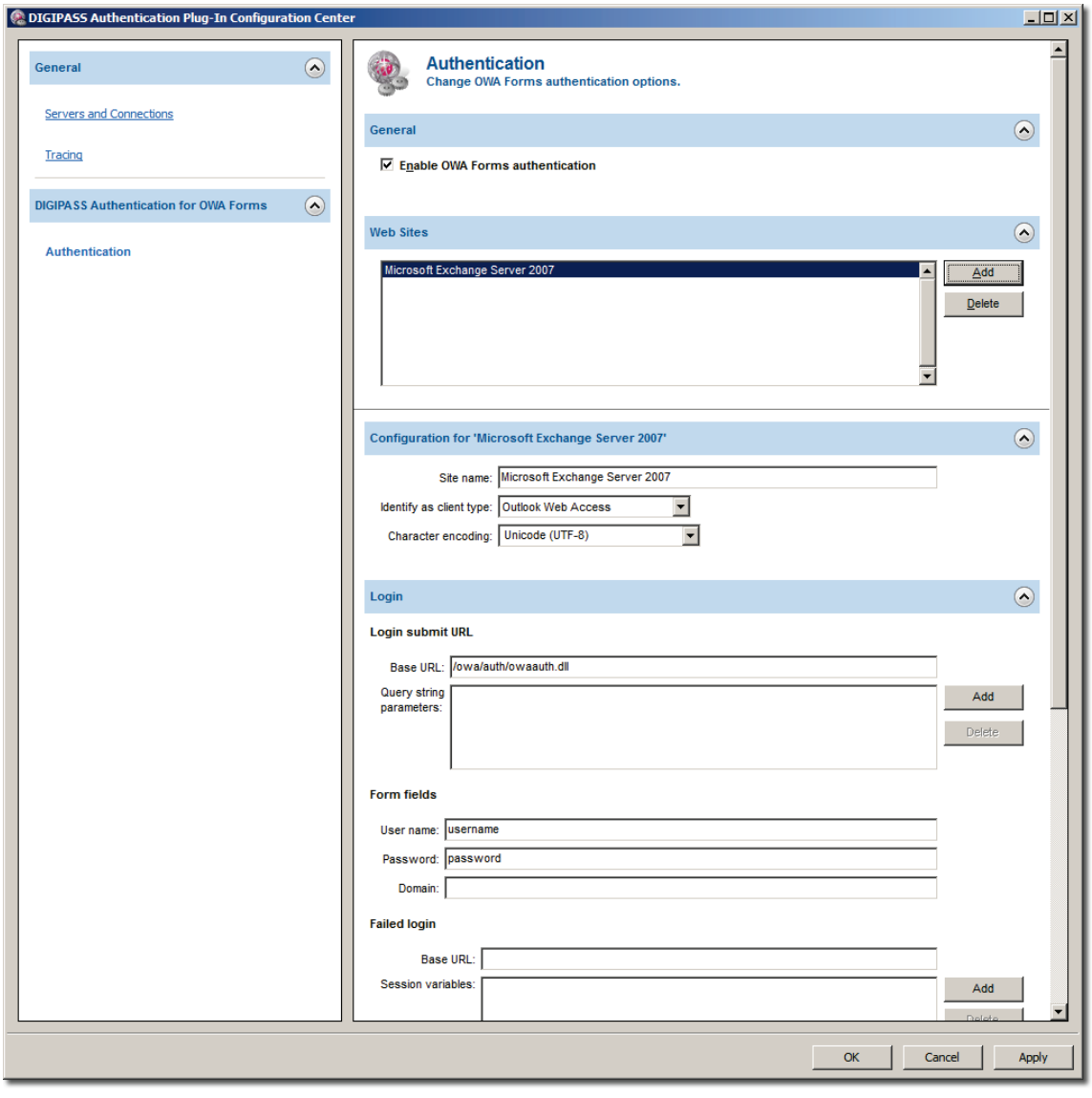

Figure 16: Configuring Authentication Settings (2)

4. Specify the settings for the Web site as needed.
   - **Site name**: Specify a name for the Web site. This name is used to distinguish the Web site in the **Web Sites** list.
   - **Identify as client type**: Select a client type from the list. The client type is used when connecting to an authentication server, to assist in finding the correct client record. The client type must match the license's client type, or authentication will not be possible.
   - **Character encoding**: Select the character encoding for HTML form parameters from the list.
5. Specify the login settings for the selected Web site.

Login submit URL

- **Base URL**: Specify the base URL.
- **Query string parameters**: Specify query string parameters for the Web site. The query string parameters list contains URL parameters required as `name=value` pairs by OWA when a login is submitted. The **DIGIPASS Authentication Plug-In** will only identify a request as a login if these variables are present in the query string.

CAUTION
You need to type the parameter exactly as it will appear in the query string.

Form fields

- **User name**: Specify the name for the user name field of the login page.
- **Password**: Specify the name for the password field of the login page.
- **Domain**: Specify the name for the domain field of the login page.

Failed login

- **Base URL**: If required, specify the base URL of the failed login page. If the **DIGIPASS Authentication Plug-In** fails to authenticate the user, the Web browser is redirected to this URL. If this field is left empty, the default OWA failure message will be displayed.
- **Session variables**: Specify session variables for the failed login page. The **Session Variables** list contains query string parameters from the login submit request which should be included in the failed login URL, such as session identifiers.
- **Return failure reason**: Select this if you want to enable the **DIGIPASS Authentication Plug-In** to add information about a login failure to the login page. Authentication failure code and reason will be included in the failed login page request. If a custom failed login page is provided, this information can be evaluated by examining the `failcode` and `failmessage` query string parameters.

Two-step challenge/response

- **Template**: Specify the location of the challenge/response template if you want to use two-step challenge/response or Virtual DIGIPASS login.

6. Specify the settings for one-step challenge/response.
   - **Enable one-step challenge/response**: Select this to allow one-step challenge/response logins.
   - **Base URL**: Specify the base URL of the login request page.
   - **Query string parameters**: Specify query string parameters for the Web site. The query string parameters list contains URL parameters required by OWA when a login is submitted. The **DIGIPASS Authentication Plug-In** will only identify a request as a one-step challenge/response login if these variables are present in the query string.

CAUTION
You need to type the parameter exactly as it will appear in the query string.

CAUTION
If a Web site is configured to use the same base URL and query string parameters for both response-only and one-step challenge/response login, the **DIGIPASS Authentication Plug-In** will not be able to distinguish between them. In this case, it will attempt to perform a one-step challenge/response authentication.

In addition, if you have multiple Web sites configured to use the same base URL and query string parameters, the topmost Web site definition in the list will take precedence for authentication.

7. Click **Apply** for your changes to take effect.

4.1.4 Configuring Tracing

➢ To configure settings for tracing

1. Start **DIGIPASS Authentication Plug-In Configuration Center** and select **Tracing**.
2. Specify the tracing level.
   For more information, refer to Section 2.5 Tracing.

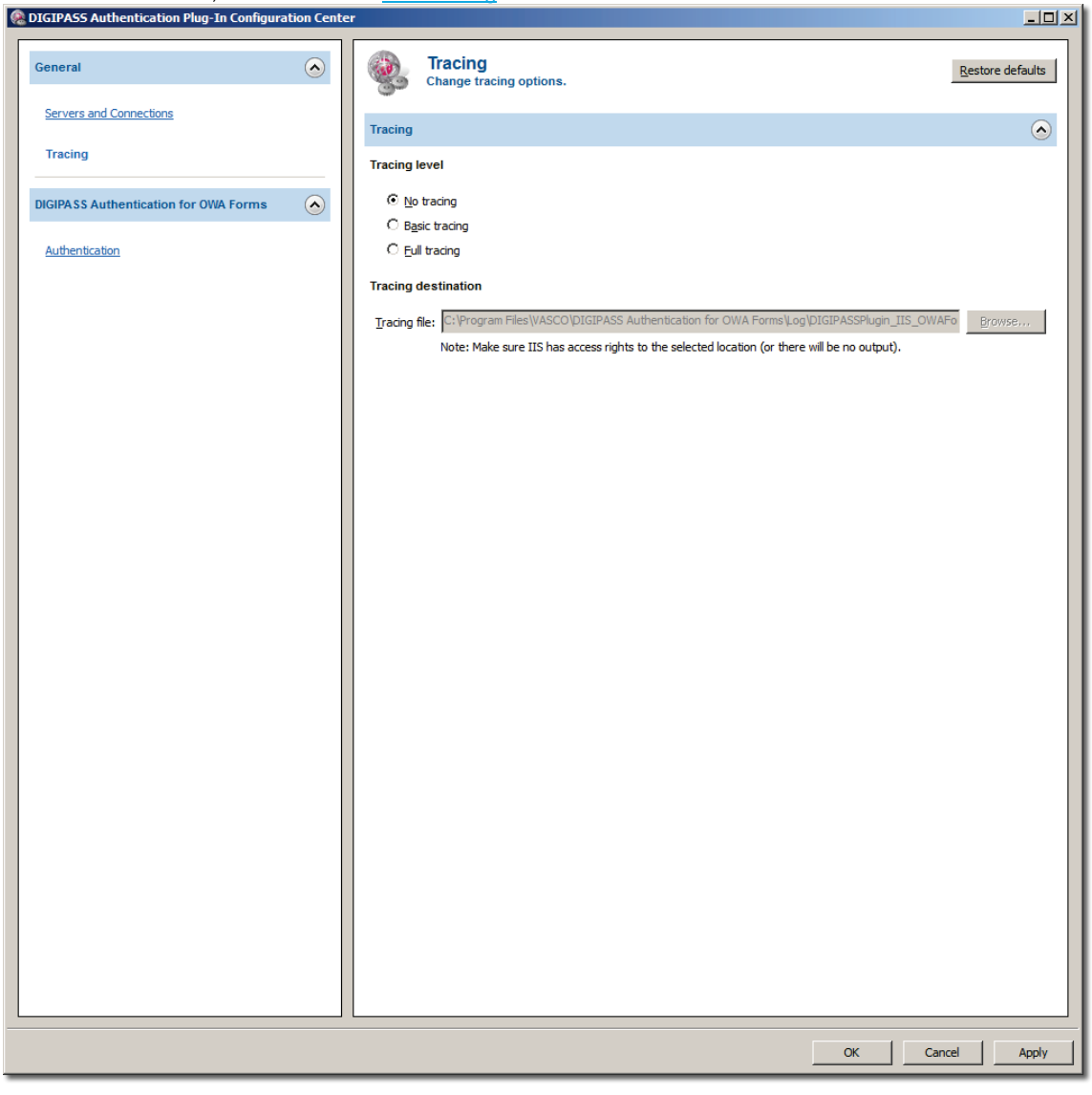

Figure 17: Configuring Tracing Options

3. If you have selected basic or full tracing, specify the path and filename for the tracing file. The file path must be the full absolute path. Relative paths may be misinterpreted in the IIS environment so that the trace file cannot be written to.

4. Click **Apply** for your changes to take effect.

4.2 Editing the Configuration File

The **DIGIPASS Authentication Plug-In Configuration Center** writes to an XML file named Settings.xml in the installation directory. It is possible to edit this file directly instead of using the **Configuration Center**.

NOTE
This option is recommended only for advanced users. The **DIGIPASS Authentication Plug-In Configuration Center** will prevent most common configuration mistakes, but there are no such checks made when edits are made directly to the configuration file. Incorrect changes to the configuration file may cause the **DIGIPASS Authentication Plug-In** to stop working.

If Settings.xml is damaged, uses incorrect XML syntax, etc., the **DIGIPASS Authentication Plug-In** will attempt to operate with default values, with logging enabled (and attempt to report the problems with Settings.xml).

4.2.1 Example Configuration File

```
<?xml version="1.0" encoding="UTF-8" ?>
<Profile>
  <Key Name="Servers and Connections">
    <Value Name="LocalIPAddress" Type="STRING">192.168.47.11</Value>
    <Value Name="ServerLoadBalancing" Type="BOOL">FALSE</Value>
    <Key Name="ConnectionList">
      <Key Name="Connection0">
        <Value Name="Name" Type="STRING">Main Server</Value>
        <Value Name="ServerIPAddress" Type="STRING">192.168.1.1</Value>
        <Value Name="ServerPort" Type="INT">20003</Value>
        <Value Name="ServerType" Type="STRING">Primary</Value>
        <Value Name="MaxConcurrentConnections" Type="INT">10</Value>
        <Value Name="ConnectionTimeoutSeconds" Type="INT">10</Value>
        <Value Name="MinReconnectIntervalSeconds" Type="INT">10</Value>
        <Value Name="MaxReconnectIntervalSeconds" Type="INT">10</Value>
        <Key Name="SSL">
          <Value Name="EnableSSL" Type="BOOL">TRUE</Value>
          <Value Name="EnableCustomCertificateArchiveFile" Type="BOOL">
           FALSE
          </Value>
          <Value Name="CustomCertificateArchiveFilePath" Type="STRING">
          </Value>
        </Key>
      </Key>
    </Key>
  </Key>

  <Key Name="Tracing">
    <Value Name="TraceFilePath" Type="STRING">
     C:\Program Files\VASCO\DIGIPASS Authentication for OWA Forms\Log
     \DIGIPASSPlugin_IIS_OWAForms.trace
    </Value>
```

```
    <Value Name="TraceFileEnable" Type="BOOL">FALSE</Value>
    <Value Name="TraceCodeInfo" Type="BOOL">FALSE</Value>
    <Value Name="TraceProcessInfo" Type="BOOL">FALSE</Value>
    <Value Name="TraceLevel" Type="INT">100</Value>
  </Key>

  <Key Name="FormsBasedAuthentication">
    <Value Name="Enabled" Type="BOOL">TRUE</Value>
    <Key Name="SiteList">
      <Key Name="Site0">
        <Value Name="Name" Type="STRING">
         Microsoft Exchange Server 2007
        </Value>
        <Value Name="ComponentType" Type="STRING">
         Outlook Web Access
        </Value>
        <Key Name="LoginRequestFields">
          <Value Name="DomainField" Type="STRING">domain</Value>
          <Value Name="UsernameField" Type="STRING">username</Value>
          <Value Name="PasswordField" Type="STRING">password</Value>
        </Key>
        <Value Name="Encoding" Type="STRING">UTF-8</Value>
        <Key Name="LoginPage">
          <Value Name="BaseURL" Type="STRING">
           /owa/auth/owaauth.dll
          </Value>
          <Key Name="QueryStringParameterList">
            <Key Name="QueryStringParameter0">
              <Value Name="NameValuePair" Type="STRING">
               param0=value0
              </Value>
            </Key>
            <Key Name="QueryStringParameter1">
              <Value Name="NameValuePair" Type="STRING">param1=</Value>
            </Key>
            <Key Name="QueryStringParameter2">
              <Value Name="NameValuePair" Type="STRING">param2</Value>
            </Key>
          </Key>
        </Key>
        <Key Name="FailedLoginPage">
          <Value Name="BaseURL" Type="STRING">
           /owa/auth/logon.aspx?replaceCurrent=1&amp;reason=2
          </Value>
          <Value Name="ReturnErrorReasonEnabled" Type="BOOL">
           TRUE
          </Value>
          <Key Name="SessionVariableList">
            <Key Name="SessionVariable0">
              <Value Name="Name" Type="STRING">sessid</Value>
            </Key>
          </Key>
        </Key>
        <Key Name="OneStepChallengeResponsePage">
          <Value Name="BaseURL" Type="STRING">
```

```
            /OWA/auth/logon.aspx
          </Value>
          <Value Name="Enabled" Type="BOOL">TRUE</Value>
          <Key Name="QueryStringParameterList">
            <Key Name="QueryStringParameter0">
              <Value Name="NameValuePair" Type="STRING">
               method=oscr
              </Value>
            </Key>
          </Key>
        </Key>
        <Key Name="TwoStepChallengeResponse">
          <Value Name="TemplateFilename" Type="STRING">
           C:\Program Files\VASCO\DIGIPASS Authentication for OWA
           Forms\Templates\Common\Challenge_template.html
          </Value>
          <Value Name="FormMethod" Type="STRING">POST</Value>
        </Key>
      </Key>
    </Key>
  </Key>
</Profile>
```

4.2.2 Configuration Settings

This section lists configuration settings and their default values. After **DIGIPASS Authentication Plug-In** installation, Settings.xml contains only a few basic settings. After the configuration wizard is completed, the file is filled with the default configuration for OWA forms.

4.2.2.1 Servers and connections

“Servers and Connections” > “LocalIPAddress”

The address from which to connect to the authentication server. The default value is the IP address automatically detected by the install program. If more than one IP address was detected, this value will be the IP address selected during installation.

“Servers and Connections” > “ServerLoadBalancing”

Enable/disable load balancing for connections to authentication servers. The default value is FALSE.

“Servers and Connections” > “ConnectionList” > “Connection0” > “Name”

The server name that will be displayed in the **Authentication servers** list in the **DIGIPASS Authentication Plug-In Configuration Center**. The default value is Main Server.

“Servers and Connections” > “ConnectionList” > “Connection0” > “ServerIPAddress”

The authentication server's IP address.

"Servers and Connections" > "ConnectionList" > "Connection0" > "ServerPort"

The authentication server's port. The default value is 20003.

"Servers and Connections" > "ConnectionList" > "Connection0" > "ServerType"

Either primary or backup authentication server. This setting affects load-balancing. The default value is Primary.

"Servers and Connections" > "ConnectionList" > "Connection0" > "MaxConcurrentConnections"

The maximum number of concurrent connections which the **DIGIPASS Authentication Plug-In** may hold open to the authentication server. The default value is 10.

"Servers and Connections" > "ConnectionList" > "Connection0" > "ConnectionTimeoutSeconds"

Connection timeout in seconds. The default value is 10.

"Servers and Connections" > "ConnectionList" > "Connection0" > "MinReconnectIntervalSeconds"

The minimum amount of time in seconds that the **DIGIPASS Authentication Plug-In** will leave between attempts to reconnect to an authentication server after an unsuccessful connection attempt (e.g. server busy). The default value is 10.

"Servers and Connections" > "ConnectionList" > "Connection0" > "MaxReconnectIntervalSeconds"

The maximum amount of time in seconds that the **DIGIPASS Authentication Plug-In** will leave between attempts to reconnect to an authentication server after an unsuccessful connection attempt (e.g. server busy). The default value is 10.

"Servers and Connections" > "ConnectionList" > "Connection0" > "SSL" > "EnableSSL"

Enable/disable the use of SSL when connecting to this authentication server. The default value is FALSE.

"Servers and Connections" > "ConnectionList" > "Connection0" > "SSL" > "EnableCustomCertificateArchiveFile"

Enable/disable certificate archive file for use instead of the Windows certificate store. The default value is FALSE.

"Servers and Connections" > "ConnectionList" > "Connection0" > "SSL" > "CustomCertificateArchiveFilePath"

File location and name of custom certificate store.

4.2.2.2 Tracing

"Tracing" > "TraceFilePath"

The absolute path and file name of the file to which internal state tracing will be written. The file but not the path will be created by the **DIGIPASS Authentication Plug-In** if it does not exist, whenever information is logged. The default value is <INSTALLATION DIRECTORY>\Log\DIGIPASSPlugin_IIS_OWAForms.trace.

"Tracing" > "TraceFileEnable"

Enable/disable tracing. The default value is FALSE.

"Tracing" > "TraceCodeInfo"

Defines if source code information is traced. Use this for troubleshooting in collaboration with VASCO support. The default value is FALSE.

"Tracing" > "TraceProcessInfo"

Defines if process information is dumped at start and end of tracing session. The default value is FALSE.

"Tracing" > "TraceLevel"

Basic or full tracing. The possible values are:

- 300 for errors only
- 200 for errors and warnings
- 100 for basic tracing
- 50 for full tracing
- 25 for full tracing including connection diagnostics information

The default value is 100.

4.2.2.3 Forms-based authentication

"FormsBasedAuthentication" > "Enabled"

Enable/disable forms-based authentication with the **DIGIPASS Authentication Plug-In**. The default value is TRUE.

"FormsBasedAuthentication" > "SiteList" > "Site0" > "Name"

Text to display in the **Web Sites** list in the **DIGIPASS Authentication Plug-In Configuration Center**. The default value is Microsoft Exchange Server 2007 or Microsoft Exchange Server 2010.

"FormsBasedAuthentication" > "SiteList" > "Site0" > "ComponentType"

The **DIGIPASS Authentication Plug-In** to use. The default value is Outlook Web Access.

"FormsBasedAuthentication" > "SiteList" > "Site0" > "LoginRequestFields" > "DomainField"

Name of the field that corresponds to domain.

"FormsBasedAuthentication" > "SiteList" > "Site0" > "LoginRequestFields" > "UsernameField"

Name of the field that corresponds to user name. The default value is username.

"FormsBasedAuthentication" > "SiteList" > "Site0" > "LoginRequestFields" > "PasswordField"

Name of the field that corresponds to password. The default value is password.

"FormsBasedAuthentication" > "SiteList" > "Site0" > "Encoding"

Character set to use in sending a login request to the Web server. If you are using non-Western European characters, the **DIGIPASS Authentication Plug-In** may need to be configured to use a specific character set when submitting login requests to the Web site. The default value is UTF-8.

CAUTION
The **DIGIPASS Authentication Plug-In** can only be configured to use a single character set – it is not able to handle multiple character sets simultaneously.

Table 1: Language Codes

Language	ISO Code	Windows Code	Other Code(s)
Arabic	ISO-8859-6	CP1256	
Baltic	ISO-8859-4 or ISO-8859-13	CP1257	
Central European	ISO-8859-2	CP1257	

Language	ISO Code	Windows Code	Other Code(s)
Chinese Simplified	ISO-2022-CN		GB2312
Chinese Traditional			Big5
Cyrillic	ISO-8859-2	CP1251	
Greek	ISO-8859-7	CP1253	
Hebrew	ISO-8859-8-I	CP1255	
Japanese	ISO-2022-JP		
Korean	ISO-2022-KR		
Thai	ISO-8859-11	CP874	
Turkish	ISO-8859-9		
Vietnamese		CP1258	
Western European	ISO-8859-1	CP1252	

“FormsBasedAuthentication” > “SiteList” > “Site0” > “LoginPage” > “BaseURL”

URL to use in submitting a login. The default value is /owa/auth/owaauth.dll (Exchange 2007) or /owa/auth.owa (Exchange 2010).

“FormsBasedAuthentication” > “SiteList” > “Site0” > “LoginPage” > “QueryStringParameterList” > “QueryStringParameter0” > “NameValuePair”

Query string parameter needed in the URL.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “FailedLoginPage” > “BaseURL”

URL to use after a failed login attempt. The default value is /owa/auth/logon.aspx?replaceCurrent=1&reason=2.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “FailedLoginPage” > “ReturnErrorReasonEnabled”

Enable/disable returning the error reason after a failed login attempt. The default value is TRUE.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “FailedLoginPage” > “SessionVariableList” > “SessionVariable0” > “Name”

Session variables for the failed login page. The **Session Variables** list contains query string parameters from the login submit request which should be included in the failed login URL, such as session identifiers.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “OneStepChallengeResponsePage” > “BaseURL”

URL to use in making a one-step challenge/response login request. The default value is /owa/auth/logon.aspx.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “OneStepChallengeResponsePage” > “Enabled”

Enable/disable one-step challenge/response logins. The default value is FALSE.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “OneStepChallengeResponsePage” > “QueryStringParameterList” > “QueryStringParameter0” > “NameValuePair”

Query string parameter needed in the URL.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “OneStepChallengeResponsePage” > “QueryStringParameterList” > “QueryStringParameter1” > “NameValuePair”

Query string parameter needed in the URL. The default value is replaceCurrent=1.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “TwoStepChallengeResponsePage” > “TemplateFilename”

Location and file name of the template to use in creating a two-step challenge/response page. The default value is <INSTALLATION DIRECTORY>\Templates\Common\Challenge_template.html.

“FormsBasedAuthentication” > “SiteList” > “Site0” > “TwoStepChallengeResponsePage” > “FormMethod”

HTML form method to use in submitting a two-step challenge/response login request. Possible values are GET or POST. The default value is POST.

4.3 Configuring Exchange to Work with the DIGIPASS Authentication Plug-In

Authentication settings in Exchange must be compatible with the **DIGIPASS Authentication Plug-In**. The following section describes how to configure Exchange for use with the **DIGIPASS Authentication Plug-In**.

4.3.1 Configuring Exchange 2007

Exchange must have forms authentication enabled, and Windows integrated authentication disabled, to allow the **DIGIPASS Authentication Plug-In** to intercept authentication requests and, where appropriate, pass them to the authentication server.

➢ To configure Exchange 2007

1. Open Exchange Management Console.
2. Expand the required server.
3. Expand **Server Configuration**.
4. Click **Client Access**.
5. Right-click **OWA** and select **Properties**.
   The **owa (Default Web Site) Properties** Dialog is displayed.

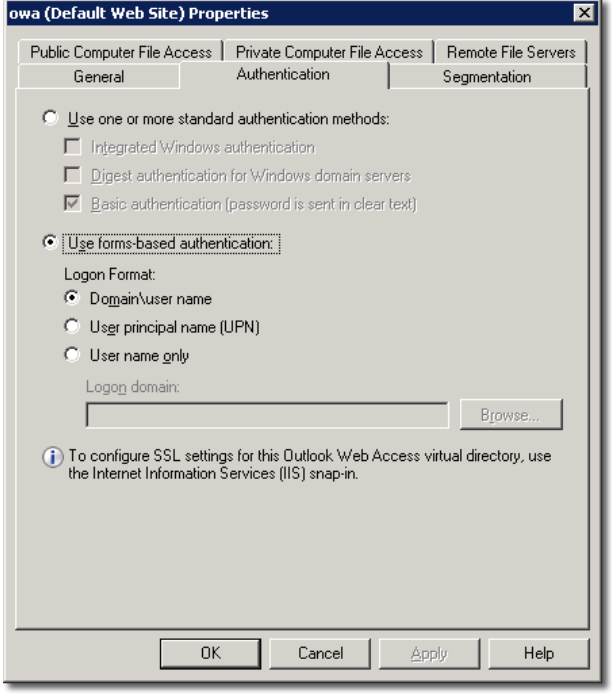

Figure 18: Modifying Authentication Settings (Exchange 2007)

6. Switch to the **Authentication** tab.
7. Ensure that **Use forms-based authentication** is selected.

> NOTE
> You may choose any of the options below **Use forms-based authentication**.

8. Click **OK**.
9. Restart the Exchange Server.

4.3.2 Configuring Exchange 2010

Exchange must have forms authentication enabled, and Windows integrated authentication disabled, to allow the **DIGIPASS Authentication Plug-In** to intercept authentication requests and, where appropriate, pass them to the authentication server.

➢ To configure Exchange 2010

1. Open Exchange Management Console.
2. Expand the required server.
3. Expand **Server Configuration**.
4. Select **Client Access**.
5. Switch to the **Outlook Web App** tab.

6. Right-click the **owa** and select **Properties**.
   The **owa (Default Web Site) Properties** Dialog is displayed.

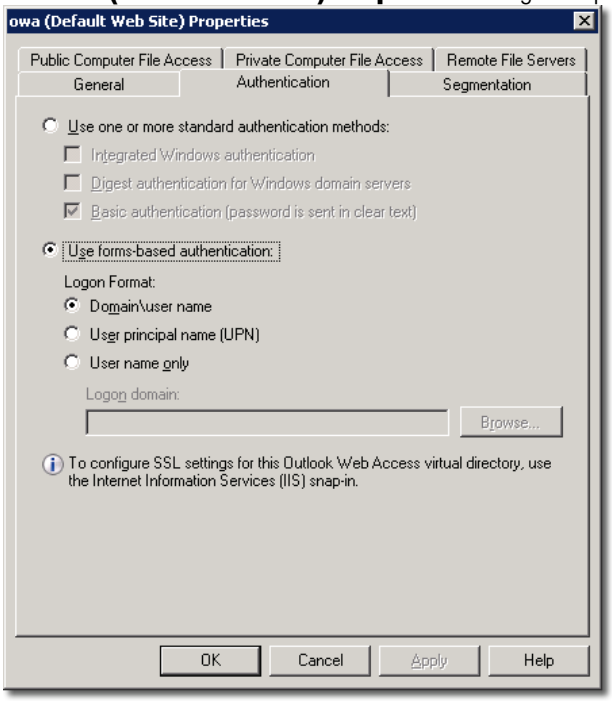

Figure 19: Configuring Exchange 2010 (1)

7. Switch to the **Authentication** tab.
8. Ensure that **Use forms-based authentication** is selected.

NOTE
You may choose any of the options below **Use forms-based authentication**.

9. Click **OK**.

10. Switch to the **Exchange Control Panel** tab.

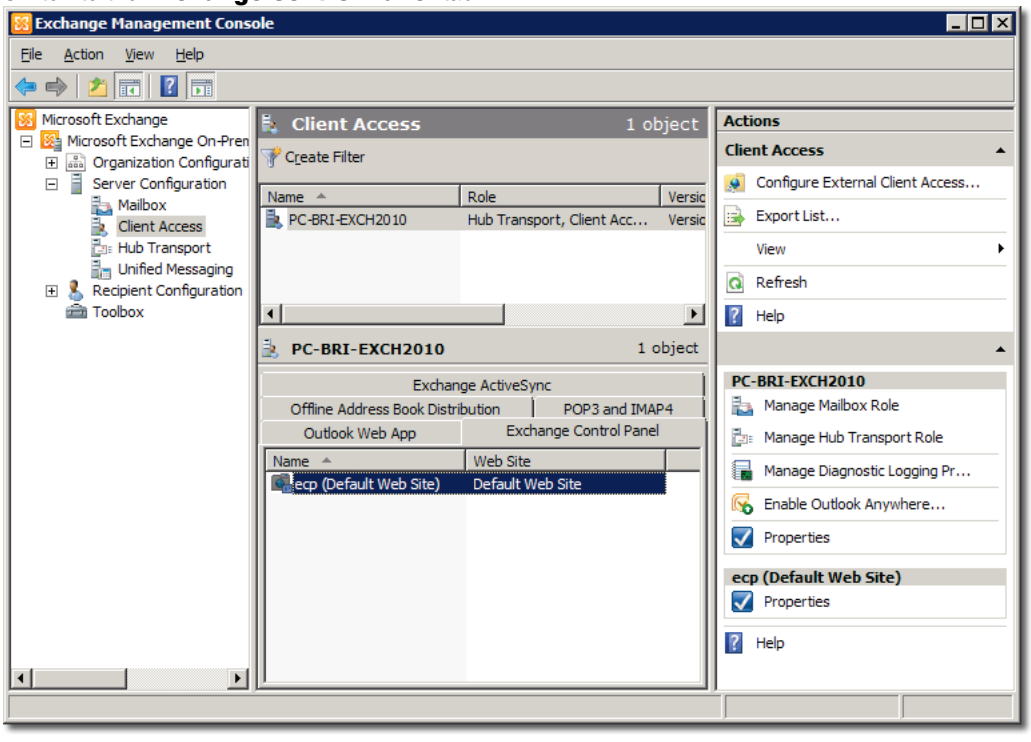

Figure 20: Configuring Exchange 2010 (2)

11. Right-click the required ECP site and select **Properties**.
    The **ecp (Default Web Site) Properties** Dialog is displayed.

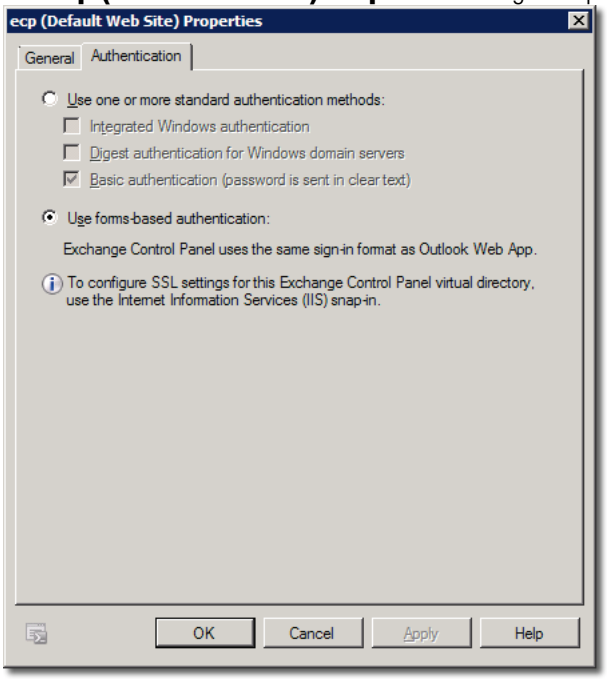

Figure 21: Configuring Exchange 2010 (3)

12. Switch to the **Authentication** tab.
13. Select **Use forms-based authentication**.
14. Click **OK**.
15. Restart the Exchange server.

4.4 Configuring the Authentication Server

4.4.1 Client Record

A client record must be configured in the authentication server for the **DIGIPASS Authentication Plug-In**. The configuration wizard can create the required record if a connection to the authentication server, and an administrator account with sufficient privileges, is available. If the configuration wizard does not create a client record, this must be done manually.

- The **Component type** should be set to Outlook Web Access.
- The **Location** should be set to the same IP address as in the **Connect from IP address** setting in the **DIGIPASS Authentication Plug-In Configuration Center**.
- Select a policy for the authentication server to use when processing authentication requests from the **DIGIPASS Authentication Plug-In**.

A valid license key must be obtained for the **DIGIPASS Authentication Plug-In** and loaded in to the client record.

4.4.2 Configuring for Windows User Accounts

4.4.2.1 Windows user name resolution

If the authentication server is installed on a Windows platform and is using an ODBC database (including the embedded database) as its data store, it is recommended that you enable Windows user name resolution. This allows the authentication server to use Windows functionality to resolve a user ID – as entered during a login – into a user ID and domain. It is highly recommended if **dynamic user registration** will be enabled.

This setting is not required where the authentication server is using Active Directory as its data store - name resolution will occur automatically.

This setting is not available on IDENTIKEY Server on Linux, or aXsGUARD Identifier.

If the **Use Windows user name resolution** feature is disabled or unavailable, it is essential that users always use the same login name. If they try to log in using a different form of their Windows account name, their login will be rejected, unless a second DIGIPASS user account has been created.

4.4.2.2 Case sensitivity

Windows user names are not case-sensitive. If the ODBC database used by the authentication server is case-sensitive, ensure that user ID case is converted to lower case. Upper case may also be used, but will involve extra configuration steps. The embedded PostgreSQL database is set to convert to lower case by default. See the Encoding and Case Sensitivity section in the IDENTIKEY Server Administrator Guide for more information.

4.4.2.3 Default domain

Where users log in without entering a domain name or UPN, the authentication server will need to be configured to use the correct domain. There are two basic scenarios that might apply:

Change master domain

If users will only ever be logging in to one domain via the authentication server, the simplest solution is to set the master domain name to the fully qualified domain name of the required domain.

This option is not available for aXsGUARD Identifier.

Set default domain in policy

This strategy should be used if:

- You wish to keep the master domain strictly for administration accounts and separate from user accounts
- The authentication server may be required to handle a different default domain for different IIS 7 Modules or other clients

Each policy may be configured with a default domain, to be used if a user does not enter a domain on login. Typically, you will need to modify the policy used by each **DIGIPASS Authentication Plug-In**.

4.4.3 Policy

The client record created during installation of the **DIGIPASS Authentication Plug-In** uses the default password replacement policy for the package. It will be named:

- IDENTIKEY Windows Password Replacement (IDENTIKEY Server)
- IDENTIKEY Microsoft AD Password Replacement (aXsGUARD Identifier)

This policy is configured with the following settings:

- Back-end authentication is set to Always (used for **dynamic user registration**, **password autolearn**, etc. Not all logins).
- Windows is used as the back-end authenticator in the IDENTIKEY Windows Password Replacement policy.
- **Dynamic user registration**, **password autolearn** and **stored password proxy** are enabled.

- Group check mode is set to Pass Back and DIGIPASS Users is placed in the **Group** list. This will mean that any logins by users not in the DIGIPASS users group will be ignored – not rejected – by the authentication server in the IDENTIKEY Windows Password Replacement policy.

If you need different settings, either select a different policy (e.g. Self-Assignment or Auto-Assignment) for the **DIGIPASS Authentication Plug-In** component or copy the password replacement policy to a new record, modify the new policy as required, and use the new policy for the **DIGIPASS Authentication Plug-In** component.

4.4.3.1 DIGIPASS users log in with OTP only (Windows user accounts)

The following settings are recommended for this scenario:

Back-end authentication

- Back-end authentication: if needed
- Back-end protocol: Windows (IDENTIKEY Server) or Microsoft AD (aXsGUARD Identifier)

These settings allow the authentication server to check user login details with Active Directory in case of **DUR**, **password autolearn** and Self-Assignment logins through the **DIGIPASS Authentication Plug-In**.

DIGIPASS user account handling

- Dynamic user registration: enabled
- Password autolearn: enabled
- Stored password proxy: enabled

These settings allow the authentication server to create an account for an unrecognized user based on a successful Windows or Active Directory authentication. The authentication server can then store the user's Active Directory password and replay it to the **DIGIPASS Authentication Plug-In** in place of the one-time password entered by the user on future logins.

DIGIPASS assignment mode

Either Self-Assignment or Auto-Assignment would typically be used in this scenario, although manual assignment may also be used.

Local authentication

The typical setting for local authentication would be DIGIPASS/Password, meaning that users usually need to use an OTP when logging in, but are not required to in some circumstances (e.g. in grace period).

4.4.3.2 DIGIPASS users log in with password and OTP (Windows user accounts)

The following settings are recommended for this scenario:

Back-end authentication

- Back-end authentication: if needed
- Back-end protocol: Windows (IDENTIKEY Server) or Microsoft AD (aXsGUARD Identifier)

These settings allow the authentication server to check user login details with Windows or Active Directory in case of **DUR** and Self-Assignment logins through the **DIGIPASS Authentication Plug-In**.

DIGIPASS user account handling

- Dynamic user registration: enabled
- Password autolearn: disabled
- Stored password proxy: disabled

These settings allow the authentication server to create an account for an unrecognized user based on a successful Windows or Active Directory authentication. The authentication server will not store or replay a user's Active Directory password.

DIGIPASS assignment mode

Either Self-Assignment or Auto-Assignment would typically be used in this scenario, although manual assignment may also be used.

Local authentication

The typical setting for local authentication would be DIGIPASS/Password, meaning that users usually need to use an OTP when logging in, but are not required to in some circumstances (e.g. in grace period).

4.4.3.3 Local authentication only

These settings are typically used where:

- The authentication server does not check authentication details against Windows accounts.

Back-end authentication

- Back-end authentication: none

The authentication server will not check user login details with Active Directory.

DIGIPASS user account handling

- Dynamic user registration: disabled
- Password autolearn: disabled
- Stored password proxy: disabled

New DIGIPASS user accounts must be created manually (no **DUR**). An Active Directory password is not stored, because back-end authentication is disabled.

DIGIPASS assignment mode

Manual assignment would be used in this scenario.

Local authentication

The typical setting for local authentication would be Digipass Only, requiring users to log in with an OTP.

4.4.3.4 One-step challenge/response

If you use one-step challenge/response, you will need these policy settings:

- One-step challenge/response permitted: yes – server challenge
- Challenge length: 4 digits
- Add check digit as required
- Challenge check mode: 0

For more information, see the Policies section of the IDENTIKEY Server Product Guide.

4.4.3.5 Two-step challenge/response

If you use two-step challenge/response, you will need these policy settings:

- Request method: as required
- Request keyword: as required

For more information, see the Policies section of the IDENTIKEY Server Product Guide.

4.4.3.6 Virtual DIGIPASS

If you use Virtual DIGIPASS login, you will need these policy settings:

- Delivery method: as required
- Primary/Backup Virtual DIGIPASS: as required
- Request method: as required
- Request keyword: as required
- BVDP mode: as required
- Time limit: as required
- Max. uses/user: as required

For more information, see the Policies section of the IDENTIKEY Server Administrator Guide.

5 Post-Installation Tasks

This chapter lists and describes tasks you need to complete after installing the **DIGIPASS Authentication Plug-In**.

This chapter covers the following topics:

- Setting Up the Response-Only Login Page
- Setting Up the One-Step Challenge/Response Login
- Displaying the Login Failure Reason
- Creating a Two-Step Challenge/Response Template

5.1 Setting Up the Response-Only Login Page

An example logon.aspx is delivered along with DIGIPASS Authentication for OWA Forms. You may create your own based on this template, use the template as is, or use the standard OWA login page. No further configuration steps are necessary.

➢ If you do not want to use the standard OWA login page

1. Backup the existing login page.
2. Copy over the existing page with the supplied login page in <INSTALLATION DIRECTORY>\Templates\OWAF <VERSION>\logon.aspx.

   -OR-

   modify the existing page with VASCO's code.

5.2 Setting Up the One-Step Challenge/Response Login

> NOTE
> This step only needs to be performed if one-step challenge/response is being implemented.

Implementing one-step challenge/response login requires the login page used by OWA to be modified. The standard OWA login page has been modified and placed in the <INSTALLATION DIRECTORY>\Templates\OWAF <VERSION> directory. To use a login page which has been customized for your company – e.g. colors and graphics used – follow the instructions in Section 5.2.3.1 Modifying the custom login page.

5.2.1 Configuring the Authentication Server

➢ To configure the authentication server

- Enable one-step challenge/response in the policy set in the **DIGIPASS Authentication Plug-In**'s client record.
  See 4.4.3.4 One-step challenge/response for policy settings required for one-step challenge/response.

5.2.2 Configuring the DIGIPASS Authentication Plug-In

➢ To configure the authentication plug-in

- Enable one-step challenge/response in the **DIGIPASS Authentication Plug-In Configuration Center**. This may be enabled for the main Web site, or in a separate Web site catering only for one-step challenge/response logins.

5.2.3 Configuring the Login Page

➢ To configure the login page

1. Backup <EXCHANGE DIRECTORY>\logon.aspx to a suitable place.
2. To use the default login page supplied with DIGIPASS Authentication for OWA Forms, copy the login page from <INSTALLATION DIRECTORY>\Templates\OWAF <VERSION>\logon.aspx to <EXCHANGE DIRECTORY>\logon.aspx.

5.2.3.1 Modifying the custom login page

If you have a current login page in use which differs from the standard OWA login page, you may need to modify it rather than replacing it with the login page provided with the **DIGIPASS Authentication Plug-In**.

When the **DIGIPASS Authentication Plug-In** detects a request for the login page, it adds the following headers to the request before passing it on:

- VASCO-Challenge: contains the string challenge to be displayed to the user, e.g. “1234”
- VASCO-State: contains data that needs to be passed as the field `VMExtState` on the login request

➢ To modify the custom login page for one-step challenge/response

1. Backup <EXCHANGE DIRECTORY>\logon.aspx to a suitable place.
2. Open logon.aspx, which is located in <INSTALLATION DIRECTORY>\Templates\OWAF <VERSION>\.
3. Copy the following piece of code to the appropriate location in your custom login file:

CAUTION
Make sure you insert the VASCO code to the correct location in the file. Refer to the example login file delivered with the **DIGIPASS Authentication Plug-In** to find out where the VASCO code needs to go in your custom login page.

```
<!-- DIGIPASS Authentication for OWA Forms modifications : START -->
<!-- The following is required for one-step-challenge response -->
<%
System.String VascoChallenge =
Request.ServerVariables["HTTP_VASCO_CHALLENGE"];
System.String VascoState = Request.ServerVariables["HTTP_VASCO_STATE"];

if(!System.String.IsNullOrEmpty(VascoState) &&
!System.String.IsNullOrEmpty(VascoChallenge)) {
%>
    <tr>
      <td nowrap><label for="vascochallenge">Challenge:</label></td>
      <td class="txtpad">
        <input id="vascochallenge" name="challenge"
         type="text" class="txt" readonly="true" value="<%=
         VascoChallenge %>">
      </td>
    </tr>
    <input name='DPExtState' type='hidden' value='<%= VascoState %>'>
<%
}
%>
<!-- DIGIPASS Authentication for OWA Forms modifications : END -->
```

4. Save and close the custom login file.

5.3 Displaying the Login Failure Reason

NOTE
This step is OPTIONAL for all installations.

The **DIGIPASS Authentication Plug-In** may be configured to pass information to OWA when it fails an authentication request. This information may be used to provide users with an explanation of why their login failed, and steps that they may be able to take to rectify the problem. The authentication server will pass the error or status code and message text for the authentication server to OWA, which may then display the message verbatim or interpret the code to provide the user with a clear explanation or set of instructions.

5.3.1 Configuring the Login Page

A simple option is to replace the default OWA login page with the one provided with the DIGIPASS Authentication for OWA Forms. This will allow OWA to display an authentication server error or status code and message on the user's screen.

➢ To display the login failure reason

1. Backup <EXCHANGE DIRECTORY>\logon.aspx to a suitable place.
2. Copy the modified login page from <INSTALLATION DIRECTORY>\Templates\OWAF <VERSION>\logon.aspx (or other location if using a custom login page) to <EXCHANGE DIRECTORY>\logon.aspx.
3. In the **DIGIPASS Authentication Plug-In Configuration Center**, select **Return failure reason** and specify the base URL of the failed login page.

5.3.1.1 Modifying the custom login page

If you have a custom logon.aspx page in use, you may need to modify it rather than replacing it with the logon.aspx page provided with the **DIGIPASS Authentication Plug-In**.

NOTE
The logon.aspx page will also be set up for one-step challenge/response. However, these portions of the page will be ignored by the **DIGIPASS Authentication Plug-In** unless one-step challenge/response is enabled in the configuration.

➢ To modify the custom login page for displaying login failure reason

1. Backup <EXCHANGE DIRECTORY>\logon.aspx to a suitable place.

2. Open logon.aspx, which is located in <INSTALLATION DIRECTORY>\Templates\OWAF <VERSION>\.
3. Copy the following pieces of code to the appropriate location in your custom login file:

CAUTION
Make sure you insert the VASCO code to the correct location in the file. Refer to the example login file delivered with the **DIGIPASS Authentication Plug-In** to find out where the VASCO code needs to go in your custom login page.

```
<!-- DIGIPASS Authentication for OWA Forms modifications : START -->
<!-- The following is required to display DIGIPASS failure reason -->
<%
System.String VascoFailCode =
System.Web.HttpUtility.UrlDecode(Request.QueryString["failcode"]);
System.String VascoFailMessage =
System.Web.HttpUtility.UrlDecode(Request.QueryString["failmessage"]);
if(!System.String.IsNullOrEmpty(VascoFailCode))
    VascoFailMessage = "(" + VascoFailCode + ") " + VascoFailMessage;

if(String.IsNullOrEmpty(VascoFailMessage))
{
%>
<!-- DIGIPASS Authentication for OWA Forms modifications : END -->
```

```
<!-- DIGIPASS Authentication for OWA Forms modifications : START -->
<!-- The following is required to display DIGIPASS failure reason -->
<%
}
else
{
%>
    <td>DIGIPASS error: <%=VascoFailMessage%></td>
<%
}
%>
<!-- DIGIPASS Authentication for OWA Forms modifications : END -->
```

4. Save and close the custom login file.

5.4 Creating a Two-Step Challenge/Response Template

The example Challenge_template.html is found in the <INSTALLATION DIRECTORY>\Templates\Common directory. You may create your own based on this template, or use the example template as is.

The template must contain a number of key words which the extension will replace with the appropriate HTML code.

> **NOTE**
> These fields may appear more than once in the file, and each instance will be replaced.

These fields are:

- `DPEXT_FORM_METHOD` - This is replaced with the configured form method. The replaced content represents the value of the method attribute of the HTML form.
- `DPEXT_FORM_ACTION` - This is replaced with the configured login submit base URL and query strings. The replaced content represents the value of the action attribute of the HTML form.
- `DPEXT_PASSWORD_FIELD_NAME` – This is replaced with the configured password field name and has to be the value of the name attribute of the corresponding HTML form field.
- `DPEXT_CHALLENGE_TEXT` - This string is replaced with the challenge issued.
- `DPEXT_HIDDEN_FIELDS` - This is replaced with any fields submitted from the login page and has to be part of the HTML form.

6 Troubleshooting

This chapter provides information about possible issues that may occur when working with DIGIPASS Authentication for OWA Forms. Read this chapter carefully as it may help you find and identify issues.

This chapter covers the following topics:

- DIGIPASS Authentication Plug-In Installation Problems
- Other Troubleshooting Options
- Repairing the Installation

6.1 DIGIPASS Authentication Plug-In Installation Problems

The installation program for the **DIGIPASS Authentication Plug-In** will usually complete the following tasks automatically. However, if it fails in these tasks for some reason, an error message will be displayed during installation. These steps can then be followed to complete the installation manually.

If you are having trouble running the authentication server and the **DIGIPASS Authentication Plug-In** for the first time, following these steps may help you track down the problem and fix it manually.

6.1.1 Checking File Placement

The following files must be placed in the directory they are listed under. If they have been moved to another directory, or incorrectly copied, the **DIGIPASS Authentication Plug-In** will not function correctly.

Table 2: Installation Structure of DIGIPASS Authentication for OWA Forms

Folders and Files	32-bit	64-bit	Description
<PROGRAMS FOLDER>\VASCO\DIGIPASS Authentication for OWA Forms			
VdsConfig32.exe	X		**DIGIPASS Authentication Plug-In Configuration Center**
VdsConfig64.exe		X	
VdsDIGIPASSPlugin_ConfigWizard32.exe	X		Configuration wizard
VdsDIGIPASSPlugin_ConfigWizard64.exe		X	Dynamic link libraries for the **DIGIPASS Authentication Plug-In Configuration Center** and the configuration wizard
DIGIPASSPlugin_IIS_OWAFormsBasedMT32.dll	X		
DIGIPASSPlugin_IIS_OWAFormsBasedMT64.dll		X	
GUI32.dll	X		
GUI64.dll		X	
ikaal3seal.dll	X	X	
libeay32.dll	X	X	
libxml2.dll	X	X	
PPDIGIPASSPlugin_Common32.dll	X		
PPDIGIPASSPlugin_Common64.dll		X	
PPDIGIPASSPlugin_IIS_FormsBased32.dll	X		
PPDIGIPASSPlugin_IIS_FormsBased64.dll		X	
ProcCore32.dll	X		
ProcCore64.dll		X	
ssleay32.dll	X	X	
StdGUI32.dll	X		
StdGUI64.dll		X	
stlport.5.2.dll	X	X	
vdsconfig.dll	X	X	
vdscore.dll	X	X	
vdscrypto.dll	X	X	
vdsdata.dll	X	X	
vdsdatamodel.dll	X	X	

Folders and Files	32-bit	64-bit	Description
vdsnetwork.dll	X	X	
vdsprocess.dll	X	X	
vdsseal.dll	X	X	
Config.sxml	X	X	Configuration file of the **DIGIPASS Authentication Plug-In Configuration Center** and the configuration wizard. NOTE: Do not edit this file!
Settings.xml	X	X	Configuration file containing settings for servers and connections, tracing, and authentication. This file is written to by the **DIGIPASS Authentication Plug-In Configuration Center** and the configuration wizard. For information about how to work with the file, refer to Section 4.2 Editing the Configuration File.
<PROGRAMS FOLDER>\VASCO\DIGIPASS Authentication for OWA Forms\1033			
String.xml	X	X	Resource files
Config.xrs	X	X	
DIGIPASSPlugin_ConfigWizard.xrs	X	X	
GUIFx.xrs	X	X	
PPDIGIPASSPlugin_Common.xrs	X	X	
PPDIGIPASSPlugin_IIS_FormsBased.xrs	X	X	
StdGUI.xrs	X	X	
<PROGRAMS FOLDER>\VASCO\DIGIPASS Authentication for OWA Forms\Documentation\1033			
DIGIPASS Authentication for OWA Forms Manual.pdf	X	X	Product documentation and license agreement
DIGIPASS Authentication for OWA Forms Release Notes.pdf	X	X	
License.pdf	X	X	
<PROGRAMS FOLDER>\VASCO\DIGIPASS Authentication for OWA Forms\Templates\Common			
Challenge_template.html	X	X	Common templates
<PROGRAMS FOLDER>\VASCO\DIGIPASS Authentication for OWA Forms\Templates\OWAF 2007			
logon.aspx	X	X	Templates for OWA 2007
Readme.txt	X	X	
<PROGRAMS FOLDER>\VASCO\DIGIPASS Authentication for OWA Forms\Templates\OWAF 2010			
logon.aspx	X	X	Templates for OWA 2010
Readme.txt	X	X	

6.1.2 Checking Permissions

6.1.2.1 Trace file directory

Permissions need to be set to allow the **DIGIPASS Authentication Plug-In** to access and write to the trace file. By default, the trace file is stored in <INSTALLATION DIRECTORY>\Log. Follow these steps for the folder the trace file will be written to.

➢ To set permissions for tracing

1. Open Windows Explorer and browse to the directory that the trace file will be written to (<INSTALLATION DIRECTORY>\Log by default).
2. Right-click on the relevant directory and select **Properties**.
   The **Log Properties** Dialog is displayed.

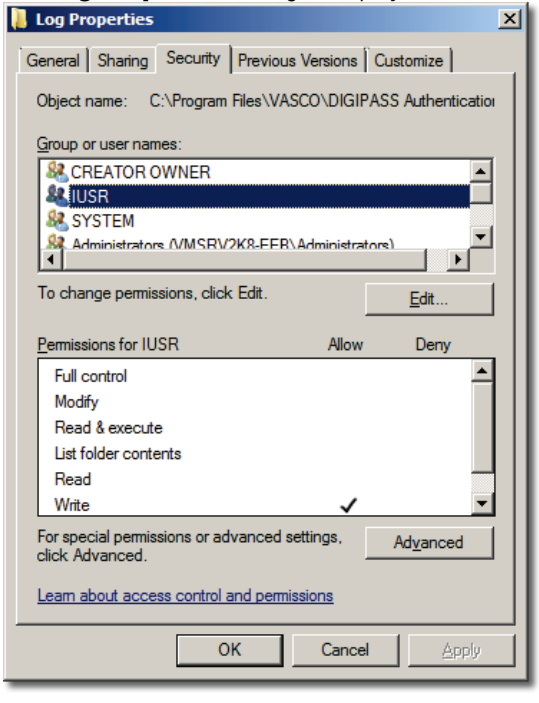

Figure 22: Setting Permissions for Tracing

3. Switch to the **Security** tab.
4. Ensure that the IUSR account has Write permissions selected.
5. Ensure that the IIS_IUSRS group has Write permissions selected.
6. If changes need to be made to the permissions, make changes and click **Apply**.

If the IIS_IUSRS group and/or the IUSR account are not listed, see Section 6.1.2.3 Adding the IUSR account and IIS_IUSRS group.

6.1.2.2 Configuration file

➢ To set permissions for accessing the configuration file

1. Open Windows Explorer and browse to the installation directory.
2. Right-click on the Settings.xml file and select **Properties**.
   The **Settings Properties** Dialog is displayed.

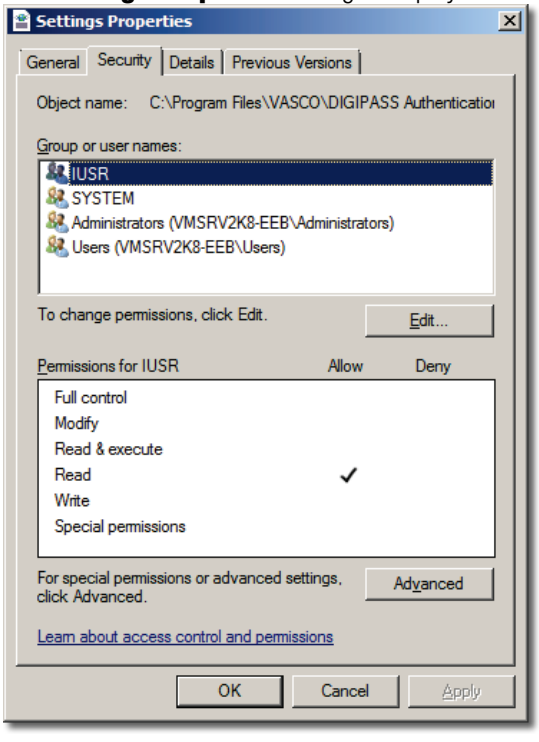

Figure 23: Setting Permissions for Accessing the Configuration File

3. Switch to the **Security** tab.
4. Ensure that the IUSR account has Read permission selected.
5. Ensure that the IIS_IUSRS group has the Read permission selected.
6. If changes were made to the permissions, click **Apply**.

If the IIS_IUSRS group and/or the IUSR account are not listed, see Section 6.1.2.3 Adding the IUSR account and IIS_IUSRS group.

6.1.2.3 Adding the IUSR account and IIS_IUSRS group

If the IUSR account and/or IIS_IUSRS group are not listed for the trace file directory or configuration file, you will need to add them.

➢ To add the IUSR account and/or IIS_IUSRS group

1. Right-click the file or directory for which you want to add the IIS_IUSRS group and/or the IUSR account and select **Properties**.
   The **<FILE/DIRECTORY> Properties** Dialog is displayed.
2. Switch to the **Security** tab and click **Edit**.
   The **Permissions for <FILE/DIRECTORY>** Dialog is displayed.
3. Click **Add**.
   The **Select Users or Groups** Dialog is displayed.
4. Type IUSR or IIS_IUSRS into the **Enter the object names to select** field and click **OK**.

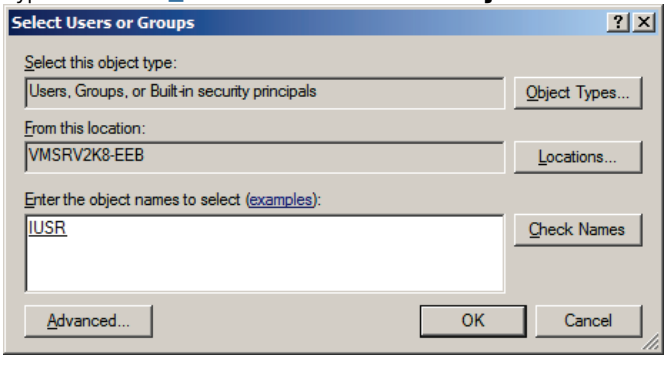

Figure 24: Adding the IIS_IUSRS Group

5. Check that the IIS_IUSRS group or IUSR user is listed.
6. Click **OK**.
   The account should now be listed in the **Group or user names** list.

6.1.3 Ensuring the DIGIPASS Authentication Plug-In Is Registered in IIS

➢ To ensure the DIGIPASS Authentication Plug-In is registered

1. Open Internet Information Services (IIS) Manager and select the appropriate server.
2. Select **Modules**.

3. Verify that DIGIPASS Authentication for OWA Forms is in the **Modules** list.

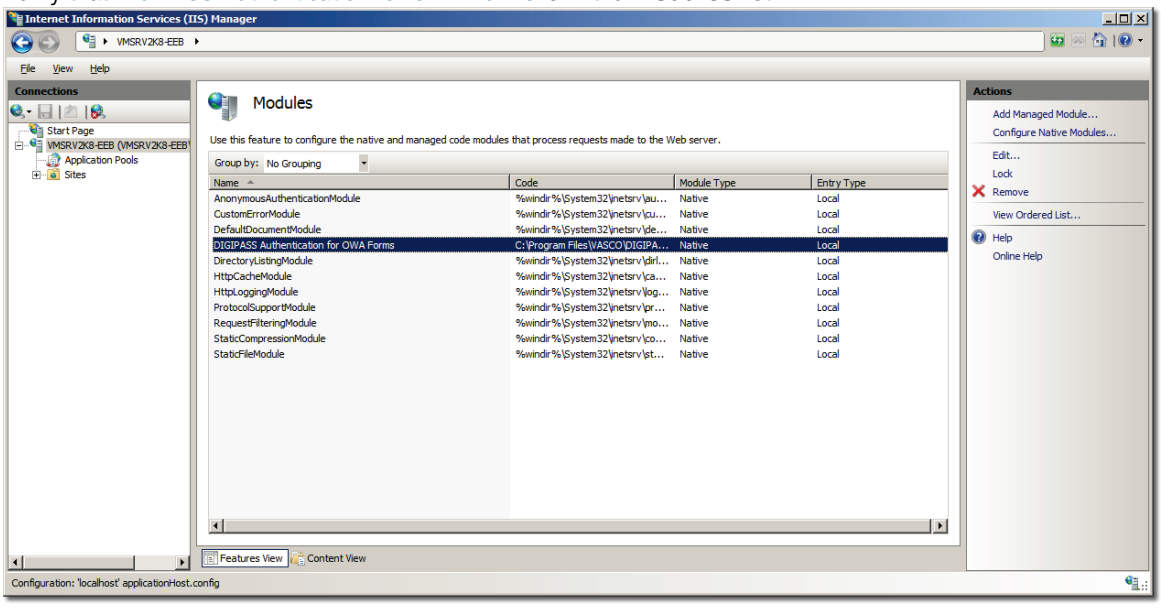

Figure 25: Ensuring the DIGIPASS Authentication Plug-In Is Registered

➢ If DIGIPASS Authentication for OWA Forms is not listed

1. In the **Actions** panel, select **Configure Native Modules**.
   The **Configure Native Modules** Dialog is displayed.

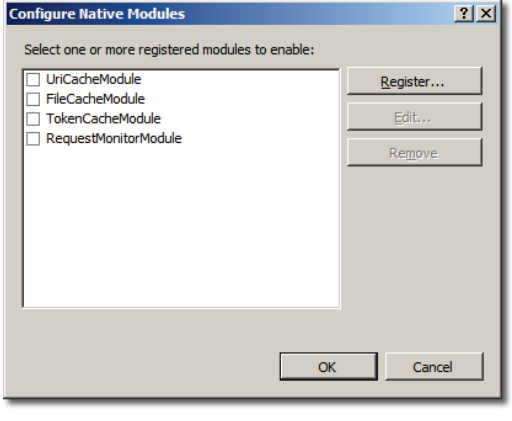

Figure 26: Registering DIGIPASS Authentication for OWA Forms in IIS (1)

2. Click **Register**.
   The **Register Native Modules** Dialog is displayed.

3. Type DIGIPASS Authentication for OWA Forms into the **Name** field, browse to<INSTALLATION DIRECTORY>DIGIPASSPlugin_IIS_OWAFormsMT32.dll (32-bit systems) or <INSTALLATION

DIRECTORY>DIGIPASSPlugin_IIS_OWAFormsMT64.dll (64-bit systems), and click **OK**.

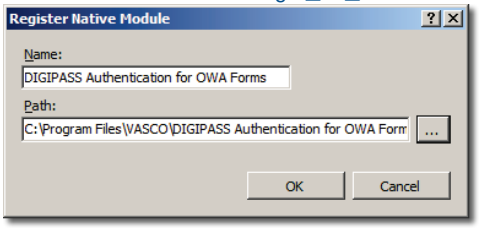

Figure 27: Registering DIGIPASS Authentication for OWA Forms in IIS (2)

4. Select DIGIPASS Authentication for OWA Forms and click **OK**.

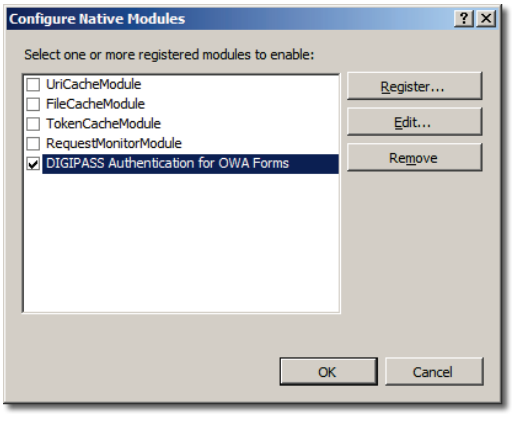

Figure 28: Registering DIGIPASS Authentication for OWA Forms in IIS (3)

DIGIPASS Authentication for OWA Forms appears in the **Modules** list.

TIP
Alternatively, to prevent performance issues, you can register the **DIGIPASS Authentication Plug-In** for specific Web sites. To do so, remove the **DIGIPASS Authentication Plug-In** from the server's **Modules** list and repeat the steps described in this section for each Web site you want to support OWA forms OTP login.

6.2 Other Troubleshooting Options

If you are still having problems after checking that all installation and configuration settings for the **DIGIPASS Authentication Plug-In** are correct, follow these steps to check for other possible problems.

6.2.1 Application Pools

If the **DIGIPASS Authentication Plug-In** stops working properly, open Internet Information Services (IIS) Manager and make sure the corresponding application pool is started. Restarting the server does not restart the application pool.

TIP
The following error message is likely to result from a stopped application pool:
"HTTP Error 503. The service is unavailable."

6.2.2 No Trace File

If there is no trace file, or no new entries are written to the file, check the Windows events for any warnings or errors generated by a failure to load the **DIGIPASS Authentication Plug-In** into IIS.

6.2.3 Information from Trace File

➢ To view trace file information

1. Set the **DIGIPASS Authentication Plug-In** to tracing.
2. Attempt a login.
3. Check the trace file for information on the start-up conditions of the **DIGIPASS Authentication Plug-In** and of the login attempt.

6.2.4 Authentication Server

If the **DIGIPASS Authentication Plug-In** appears to load and update but you are unable to achieve a successful login, check the authentication server. Open the **Audit Viewer** to:

- check available audit messages in the audit files or database.
- configure a live audit connection from the authentication server and retry a login.

See the authentication server's Administrator Reference or Administrator Guide for more information.

6.2.5 Web Browser

If you experience login problems that occur in Windows Internet Explorer only, i.e. login is possible in other Web browsers, you may need to delete the IE browser history, the corresponding cookies, and temporary files.

6.2.6 Licensing

Check that the **DIGIPASS Authentication Plug-In** has a valid client record in the authentication server data store, which has a valid license loaded. Make sure the configured local IP address and component type correspond to the client record. See the Licensing section of the authentication server's Administrator Reference or Administrator Guide for more information on licensing options.

6.2.7 SSL

If the **DIGIPASS Authentication Plug-In** is configured to use a custom certificate archive, permission issues may cause a communication error with an IDENTIKEY Server. Check that the IUSR account and IIS_IUSRS group have read permission on the configured file.

6.3 Repairing the Installation

The installation of the **DIGIPASS Authentication Plug-In** may need to be repaired if files have been corrupted, deleted or lost.

➢ To repair the DIGIPASS Authentication Plug-In installation

1. Locate and double-click on the DIGIPASS Authentication for OWA Forms.msi file.
2. Click **Next**.
3. Select **Repair** to enter the repair function and click **Next**.

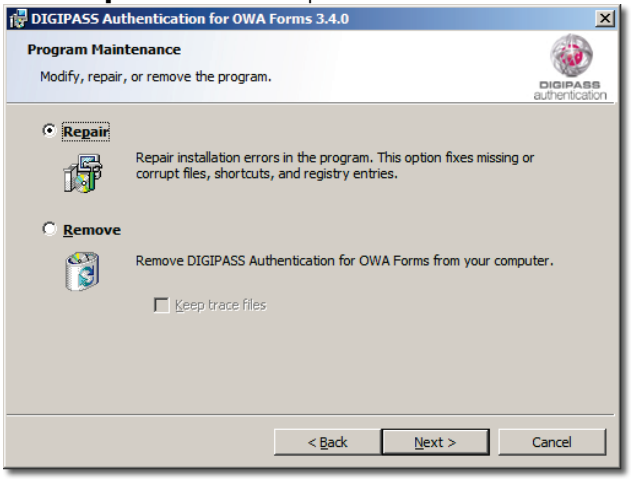

Figure 29: Repairing the Installation

4. Click **Install** to confirm the repair.
5. Click **Finish** to exit the setup program.

If you have deleted or moved the configuration file, changed the IP address for the machine or received a new license for the **DIGIPASS Authentication Plug-In**, you will need to run the DIGIPASS Authentication for OWA Forms configuration wizard after the installation repair.

7 Uninstalling DIGIPASS Authentication for OWA Forms

This chapter contains instructions to remove an existing DIGIPASS Authentication for OWA Forms installation.

This chapter covers the following topics:

- Uninstalling DIGIPASS Authentication for OWA Forms

7.1 Uninstalling DIGIPASS Authentication for OWA Forms

➢ To uninstall DIGIPASS Authentication for OWA Forms

1. Locate and double-click on the DIGIPASS Authentication for OWA Forms.msi file.
2. Click **Next**.
3. Select **Remove**.
4. Select **Keep trace files** if you want to preserve existing trace files.

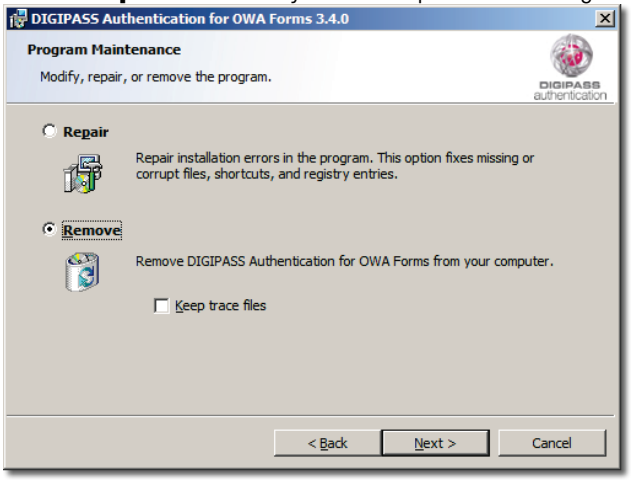

Figure 30: Removing DIGIPASS Authentication for OWA Forms

5. Click **Next**.
6. Click **Remove** to confirm the remove function.
7. Click **Finish** to exit the setup program.
8. After uninstallation, restart the system.

8 Technical Support

If you encounter problems with a VASCO product please do the following:

1. Check whether your problem has already been solved and reported in the Knowledge Base at the following URL: http://www.vasco.com/support.
2. If there is no solution in the Knowledge Base, please contact the company which supplied you with the VASCO product.

   If your supplier is unable to solve your problem, they will automatically contact the appropriate VASCO expert.

Index